Governing Identified Shadow IT by Allocating IT Task Responsibilities

Abstract

The IT unit is not the only provider of information technology (IT) used in business processes. Aiming for increased performance, many business workgroups autonomously implement IT resources not covered by their organizational IT service management. This is called shadow IT. Risks and inefficiencies associated with this phenomenon challenge organizations. Organizations need to decide how to deal with identified shadow IT and if the business or the IT unit should be responsible for corresponding tasks and components. This study proposes design principles for a method to control identified shadow IT following action design research in four organizational settings. The procedure results in an allocation of IT task responsibilities between the business workgroups and the IT unit following risk considerations and transaction cost economics, leading to an IT service governance. This contributes to governance research regarding adaptive and efficient arrangements with reduced risks for business-located IT activities.

Keywords

Shadow IT, IT Service Governance, Task Allocation, IT Risk, Transaction Cost Economics.

Introduction

More than 65% of managers acknowledge the existence of shadow IT (Chejfec 2012). This occurs as business workgroups follow their own implementation of information technology (IT) outside of formal IT processes (Behrens 2009). Today, tech-savvy users and easy access to web-based solutions increase the significance of these activities (Rentrop and Zimmermann 2012). Shadow IT, as a kind of workaround system (Alter 2014), promises flexibility and performance gains for a business and may encourage innovation (Behrens 2009). However, the violation of IT norms (Haag and Eckhardt 2014) and occurrence of risks and inefficiencies (Behrens 2009) form a managerial burden and define the need for conceptual support. Surveys show that more than 50% of IT managers are concerned about mission-critical shadow IT and possible breakdowns (Smyth and Freeman 2007). To address these concerns, this study aims at design principles for a method to handle any identified shadow IT in business workgroups.

Processes in research and practice point to IT governance to approach this goal (Györy et al. 2012; Zimmermann et al. 2014). Studies describe a broad spectrum of organizational behavior to handle shadow IT, involving further accountability in the business, a handover of partial tasks (such as server maintenance or application programming) to the IT unit, or a complete transfer to the IT unit including a possible replacement of software (Beimborn and Palitza 2013; Chua et al. 2014). While researchers are aware of the resulting task sharing, a theory-based, practical procedure on how to approach the allocation in the optimum way does not yet exist. Our research addresses this gap by presenting principles, based on action design research (ADR) (Sein et al. 2011), to allocate the task responsibilities of identified shadow IT between a business workgroup and the IT unit. Thereby, we enhance an earlier version of this paper (Zimmermann et al. 2016) by providing a more specific discussion of findings, additional details of the research method, and new implications. Following task analysis and synthesis (Picot 1990), we design a task allocation procedure by considering shadow IT and workaround risks (Alter 2014) and by applying...
transaction cost economics (TCE) (Williamson 1985). The resulting IT service governance contributes to the governance discussion on IT task responsibilities (Winkler and Brown 2014).

The following chapter formulates the problem and the resulting research question. Based on the ADR approach, we present the chosen organizational settings and theoretical basis. Next, we describe and discuss the results from the study. The study closes with conclusions and directions for further research.

**Formulating the Problem of Managing Shadow IT**

Organizations started to transfer the usage of IT and minor development tasks to end users in the 1980s. While management initiated this and was fully aware of end-user computing (EUC), over recent decades, users have started to deploy IT resources without this awareness resulting in a large-scale non-transparent IT (Ferneley 2007). The term shadow IT describes this phenomenon¹. Research defines shadow IT as IT solutions autonomously deployed in business departments to support their processes and not embedded in the organizational IT service management (Zimmermann and Rentrop 2014). Typical occurrences are installed software (Silic and Back 2014), applications based on EUC (Panko and Port 2013), self-programmed applications, cloud services (Zainuddin 2012), mobile devices (Beimborn and Palitza 2013), self-sourced hardware, and combinations thereof (Zimmermann and Rentrop 2014).

Shadow IT relates to workarounds, which present deviations from existing work systems (Alter 2014). While recent approaches address an individual’s shadow IT usage (Haag and Eckhardt 2014), this study focuses on shadow IT implemented by business workgroups in corporate IT using companies. This shadow IT mainly results from emerging IT needs in combination with a perceived lower expenditure compared with a formal implementation (Alter 2014; Györy et al. 2012; Zimmermann and Rentrop 2014). The underlying need can result from an inadequate formal IT (Jones et al. 2004). Users perceive a relative advantage in looking for alternatives (Haag 2015). Finally, they implement shadow IT if a formal solution seems too expensive and time-consuming compared with their own, hidden implementation (Behrens and Seda 2004). Perceived transaction and production costs in the relation of business and IT units dictate these considerations (Winkler and Brown 2014; Zimmermann and Rentrop 2014). Available IT resources and expertise in the business reflect preconditions (Behrens and Seda 2004; Chua et al. 2014).

Shadow IT challenges include inefficient and nonprofessional implementation (Jones et al. 2004; Panko and Port 2013), security risks (Haag 2015; Silic and Back 2014), and compliance issues (Gozman and Willcocks 2015). At the same time, it enables adaptability and user-driven innovation (Behrens 2009; Zainuddin 2012). While previous studies introduced steps to evaluate these effects (Fürstenau and Rothe 2014; Zimmermann et al. 2014), a comprehensive approach for handling identified shadow IT is not apparent, thereby challenging IT management. In the context of IT governance, which specifies accountability to increase IT control (Weill and Ross 2004, p. 8), several criteria seem to require a specific control of shadow IT (Tiwana 2009). As shadow IT can be valuable (Alter 2014; Behrens 2009; Györy et al. 2012), the necessity of forbidding business-located IT is doubtful. Moreover, shadow IT is evidence of available IT resources and knowledge present in the business. In contrast, it is understandable that IT managers, are prejudiced against business-located IT (Györy et al. 2012). In terms of risk reduction and efficient and adaptive governance (Williamson 2005), organizations need to solve these challenges.

A possible solution is to reallocate responsibilities and share the tasks of identified shadow IT between the business and the IT units (Chua et al. 2014). Regarding this allocation, researchers recently addressed the different involvement of business and IT units in IT task responsibilities (Winkler and Brown 2014). The researched spectrum of organizational behavior to handle shadow IT occurrences supports this approach of task sharing (Beimborn and Palitza 2013; Chua et al. 2014; Zimmermann et al. 2014). While research has shown the existence of these governance arrangements, no studies exist that cover a guided application of the underlying task-sharing method. However, it does seem necessary that organizations should be able to decide which task allocation is reasonable. This leads to the study’s research question:

¹ We reviewed literature to build a basis for our research. We queried EBSCOhost, ScienceDirect, IEEE Xplore, AISeL, Jstor based on abstract, title, and keywords. Employing the four-eye principle, we removed duplicates and irrelevant papers. The terms shadow IT, shadow systems, feral systems, gray IT, rogue IT, and hidden IT combined with IT, information services, information systems, and information security resulted in 27 papers. We conducted a backward and a forward search to avoid missing references.

---

**Twenty-second Americas Conference on Information Systems, San Diego, 2016**
How should organizations allocate IT task responsibilities for identified shadow IT instances between a business workgroup and the IT unit?

Action Design Research

To address this question, we use ADR that combines design research and action research and aims to generate prescriptive design knowledge through building and evaluating IT artifacts. It deals with two seemingly disparate challenges: (1) addressing a problem situation encountered in an organizational setting by intervening and evaluating and (2) constructing and evaluating an IT artifact (Sein et al. 2011). Our research goal links to these challenges. Using an action research project, we address the control of identified shadow IT in four organizational settings and, following design science, aim at constructing and evaluating a method (Braun et al. 2005) as our artifact. Choosing ADR is particularly appropriate as shadow IT is a complex phenomenon and managing it means considering several perspectives. ADR provides a way to address this, as it assumes that valid knowledge comes from various sources and the insights of researchers and practitioners are relevant to successful research (Mooney and Church 2012).

ADR follows several stages (Sein et al. 2011). The first stage is problem formulation. We formulated our problem based on literature as discussed above. It focuses on the governance challenge for organizations of controlling identified shadow IT tasks when allocating IT task responsibilities. Coupled with initial empirical investigations, we were also able to determine the scope, roles, and practitioner participation. Therefore, it became more and more evident due to several influencing, complex criteria of shadow IT that a selection of more than one organizational setting would be necessary. In the ADR approach, the use of several settings also provides a way to overcome the element of chance when receiving the insights of participating knowledge workers (Myers and Venable 2014). The consideration of multiple settings is often more convincing, as discussed in literature on case study research (Yin 2014). This resulted in an ADR procedure concentrating on different processes in four organizations. Related theories as justificatory knowledge provided a further basis for creating the new artifact and for the second ADR stage with an iterative process of building the artifact, intervention in the organization, and evaluation (BIE) (Sein et al. 2011). We describe this in the four organizational settings, focusing on different theory-based aspects of task allocation for identified shadow IT. Next, in the reflection and learning stage, we discuss the results. Finally, we generalize the learning and the gained knowledge (Sein et al. 2011).

Four Organizational Settings for Practice-inspired Research

To constitute the selection of the organizational settings with regard to the ADR principle of practice-inspired research, we used the insights from literature on case study research (Yin 2014, p. 57). We selected different business processes (Table 1) in four companies from various industries and started an ADR project one after another to achieve an iterative refinement of our artifact. We conducted the cases between July 2012 and June 2014, each spanning 3 to 4 month. We aimed for variation in the case selection to provide more valid results, i.e., the chosen processes and underlying IT requirements were standardized in Company A but very compliance and security critical; in Company B, highly business-specific, and in Company C they were affected by high uncertainty owing to rapidly changing conditions. Finally, our choice of Company D allowed a more robust evaluation, as the company had previous experience in governing shadow IT. Participants from this company served as experts (Flick 2009).

All projects were built on prior identified shadow IT. Authorized by the management, principles should be derived to control the occurrences. We identified three stakeholders within the organizational settings: Management, IT units, and the business workgroups with shadow IT. In each company, the management appointed one project manager from the IT unit who, together with in each case three researchers, formed the ADR team for building the artifact. Participants from the business and IT units served as end users, contributed to the build process, and evaluated the design. As sources of evidence within the BIE procedure, we used data from prior semi-structured interviews and surveys conducted during the shadow IT identification process, documents, technical artifacts, and contextual observations. The instances represented user-developed solutions and applications from external suppliers (such as cloud services). Further interviews, group discussions, and assessment and feedback loops with the participants supported the BIE iterations in each company (Table 1). In addition, ADR team members discussed the results with the management board to receive feedback. We started the succeeding ADR projects based on initial concept designs at the different developmental stages. The theoretical grounding for these follows.
Governing Identified Shadow IT

Prior research on application governance proves the benefit of the involvement of both business and IT units in IT task execution (Winkler and Brown 2014). Based on this, a shared involvement of business and IT units to control a prior shadow IT service defines an IT service governance. To define the degree of involvement and allocate task responsibilities, we focused on several steps.

To validate the allocation, an initial structuring of IT tasks was necessary. Following task analysis and synthesis (Picot 1990, p. 748), the structuring of an overall shadow IT instance to sub-tasks progressed according to characteristics such as the involved objects (service components like applications, database, or infrastructure) and the type of execution (tasks like developing, testing, documenting, supporting), as shown in Figure 1. The succeeding synthesis joins tasks to structured units and allocates these to individuals or workgroups. We applied this to the allocation of IT task responsibilities for shadow IT.

The risk considerations of shadow IT, described in the problem formulation, form one basis for the execution of this allocation (Chua et al. 2014; Zimmermann et al. 2014). These considerations refer to the underlying theory of workarounds and define the creation of hazards or errors, impacts on subsequent activities, and regulation issues (Alter 2014, p. 1052). Internal risk of not achieving strategic goals, security problems, and compliance issues may result. With respect to risk analysis, the high impact of a shadow IT on organizational goals and relatively low quality of such an instance leads to high internal risk, which will need to be addressed by the organization (Zimmermann et al. 2014).

When addressing inefficiencies (Alter 2014, p. 1052), the relation between the business and the IT units when exchanging IT services justifies the application of TCE (Zimmermann and Rentrop 2014). As stated in (Winkler and Brown 2014, p. 21) "Business units either enter into a contract with (...) IT units (...) or coordinate (...) operations hierarchically". In the business/IT relationship, transaction costs exist for processing and organizing the exchange of an IT service, in addition to its production cost. Experience from practice shows that business workgroups will obtain shadow IT if they assume the total cost of

---

Table 1. Organizational Settings (Company profiles all anonymized)

<table>
<thead>
<tr>
<th>Company</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
<td>Insurance</td>
<td>Engineering</td>
<td>Electronics</td>
<td>Finance</td>
</tr>
<tr>
<td>Country</td>
<td>Switzerland</td>
<td>Germany</td>
<td>Germany</td>
<td>Germany</td>
</tr>
<tr>
<td>Staff</td>
<td>1,300</td>
<td>11,500</td>
<td>5,500</td>
<td>500</td>
</tr>
<tr>
<td>Selected processes</td>
<td>Benefits Statements</td>
<td>Order Management</td>
<td>Corporate Marketing</td>
<td>Risk Management &amp; Reporting</td>
</tr>
<tr>
<td>Shadow IT</td>
<td>6 instances</td>
<td>52 instances</td>
<td>41 instances</td>
<td>102 instances</td>
</tr>
<tr>
<td>Project owner</td>
<td>Management</td>
<td>Management</td>
<td>Management</td>
<td>Management</td>
</tr>
<tr>
<td>Participants</td>
<td>2 Department heads; 1 IT manager</td>
<td>2 Department heads; 3 Employees; 1 Site director; 5 IT managers; 1 CIO</td>
<td>3 Department heads; 3 IT managers</td>
<td>10 Business team heads; 5 employees; 1 Division head; 3 IT managers</td>
</tr>
</tbody>
</table>

---

Theory-ingrained Artifact: Allocating Task Responsibilities for Shadow IT Based on Risk and Transaction Cost Economics

Figure 1. IT Task Analysis and Synthesis for a Shadow IT Instance
applying a formal service to be higher than the initial production costs for own-implementation (Zimmermann and Rentrop 2014). However, bounded rationality and opportunism (Williamson 1985, p. 30) influence this assumption and the business neglects own governance costs. Solely allocating tasks to the business may be inappropriate (Weill and Ross 2004, pp. 134–136; Zimmermann and Rentrop 2014).

TCE can be used to overcome this issue (Winkler and Brown 2014; Zimmermann et al. 2014). Its logic provides alternative governance modes to decide whether services should be produced internally or externally (Williamson 2005). This means that with regard to the business/IT exchange relationship and identified shadow IT, business workgroups can either keep IT tasks and components or obtain them from the IT unit. Thus, the procedure enables a sharing of tasks for the required IT service forming a hybrid governance mode of co-operation (Powell 1990). TCE support the decision regarding such arrangements and determine whether an internal service task allocation or one from the IT unit (external from a business view) is more beneficial (Williamson 2005). Thereby, the theory aims for optimizing the total internal and external costs in the relationship. Several cost drivers are involved.

Asset specificity influences the relationship between external and internal costs (Williamson 1985, pp. 52–54). An increasing specificity implies a more specialized investment. Production costs for an exchange partner rise as reusability for other customers declines. External transaction costs rise compared with internal governance costs owing to more complex exchange processes. In total, internal coordination becomes more efficient. This is also applicable to the business IT relation (Winkler and Brown 2014).

Environmental uncertainty is another relevant TCE dimension. It implies that “environment is characterized by uncertainty with respect to technology, demand, local factor supply conditions, inflation, and the like” (Williamson 1985, p. 336) and is important for shadow IT, which often starts as a prototype with uncertain requirements (Györy et al. 2012; Zimmermann and Rentrop 2014). Uncertainty moderates the influence of asset specificity on internal and external costs (Williamson 1985). In case of non-specific assets, uncertainty has no effect. If specificity rises, external costs increase, e.g., negotiating becomes more complex, and internal organization becomes more efficient. This is in particular relevant for a mixed specificity “incorporating standardized and customized elements” (McIvor 2009) and a high uncertainty.

Finally, frequency describes the recurrence of transactions and moderates the influence of specificity on arrangements (Williamson 1985). From an IT perspective, an appropriate determination of this dimension is the scope of use of an IT service (Winkler and Brown 2014). A higher scope increases the IT unit involvement in task responsibilities based on costs and risk considerations (Winkler and Brown 2014). We take the concepts discussed in this section into account during the development of the artifact.

Building, Intervention and Evaluation

The theoretical concepts presented in the previous section provided us with a preliminary artifact design. We further shaped the principles behind this by applying them in the four companies and in subsequent design cycles (Sein et al. 2011). We subsequently present this process by focusing on different constructs.

Risk in Company A

Swiss insurance Company A started the project in their Benefit Statements department to control six shadow IT instances. The ADR team applied the initial design. Application results defined a complete task transfer to the IT unit for two of the instances due to internal security and compliance risks. Participants tended for example to re-engineer a EUC tool-based workflow system by the IT unit. This provided evidence on how companies can deal with shadow IT risk. Two further instances remained in the business due to low relevance and no perceived cost benefit. However, IT participants claimed the necessity of documentation and maintenance. For the two remaining instances, participants pursued a balance between complete and no transfer. This assumed the involvement of both the business and IT units.

The participants evaluated the general approach in the ADR project as positive. An interviewed IT manager stated, “It is helpful to regard the relevance of a shadow IT instance in considering internal IT system risk and cost aspects to decide if the IT unit needs to adopt the service. Not all solutions need to be necessarily delivered by the IT unit.” One of the interviewed business department heads agreed with this, “The idea of the approach provides a better basis to allocate responsibilities for former shadow IT.” Based on this feedback and as we could not clearly explain the arrangement in between the two
alternatives of transferring the whole instance to the IT unit or retaining it in the business, we refined the method. We introduced a task analysis and synthesis to build a basis for a hybrid involvement of business and IT units. To advance this for a larger number of shadow IT we started an ADR project in Company B.

**Specificity and Scope of Use in Company B**

Company B executed the ADR project on the order management process of a German manufacturing plant belonging to a corporate group. Of the 52 identified shadow IT instances, 32 required a task reallocation. All remaining instances stayed in the business unit due to low risks and no expected cost benefits. However, these were registered with the IT service management for transparency reasons. For the reallocation, participants were able to cluster and integrate solutions with similar functionalities. As participants often regarded a total transfer of shadow IT tasks to the IT unit as inappropriate, we used our approach to find reasonable sharing of tasks. Thereby, the investigated shadow IT in Case B enabled us to focus (besides risk considerations as used in Company A) on the TCE dimensions of IT task specificity and scope of use, while uncertainty was principally low and less relevant.

Table 2 reflects a typical example this. The Table contains the structuring of tasks and components (see Figure 1) as well as the responsibility allocation between the business and IT unit. In general, besides tasks with high risks, non-specific tasks as well as tasks with a mixed specificity were transferred to the IT unit due to standardization and reusability reasons. Furthermore, if IT tasks remained in the business, a large scope of use required a consultation with the IT unit to ensure efficiency and further risk reduction. Participants valued this procedure highly for reducing risks and inefficiencies due to shadow IT. With regard to the described instance in Table 2, the department head of the business workgroup appreciated that “it is more reasonable to transfer server and database administration, as well as access control tasks and interface management to the IT unit to reduce risks and to use synergies.” The IT unit supported this allocation for specificity, quality, and flexibility reasons. To improve this stage and to expand the focus on the uncertainty construct, we started an ADR project in Company C.

<table>
<thead>
<tr>
<th>Shadow IT</th>
<th>IT service governance explanation</th>
<th>Specified task responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order processing program consisting of a self-developed web-based application, with a database, hosted on an externally provided server. The engineering unit developed it to process orders with drawings, calculations, &amp; scheduling.</td>
<td>Due to non-acceptable security risks and standardization, database- &amp; server-related tasks as well as access control procedures were transferred to the IT unit. In addition, participants transferred interface programming to the IT unit based on the business requirements due to a mixed specificity (standardized and customized elements) but a low uncertainty. Other tasks stayed in the business because of a high specificity; specific skills for programming drawings, calculations, etc. However, for these tasks it is necessary to consult with the IT unit due to a broad scope of use.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 2. Shadow IT instance in Company B with shared task responsibilities**

**Uncertainty in Company C**

The German electronics Company C has experienced intense growth in recent years. Business units have developed shadow IT on a large scale. Management was searching for an approach to deal with this. We started the ADR project in the Marketing Department. Due to flexibility, fast changing environment, and time to market, as well as assumed high cost when using the IT unit, marketing workgroups implemented shadow IT to test IT ideas or solutions. In the beginning, the implementation was often uncertain regarding requirements and future usage following on the changing external conditions. This influenced the allocation of IT service tasks, especially those with mixed specificity, and enabled us to provide evidence for the uncertainty construct in our method design. Table 3 provides a typically example of this.
Both business and IT staff agreed that the governance arrangements, as described in Table 3, were reasonable. A member of the IT unit stated, “There is no necessity to spend resources from the IT unit’s side until the business is certain about future usage. If it is more certain it will become for example the task of the IT unit to provide an appropriate interface to core systems.” Besides this initially complete task allocation to the business, other instances exceeded the limits of uncertainty. For these, a reallocation of service tasks took place according to risk, specificity, and scope of use. Similar to Company B, infrastructure and database components were centralized. Of the 41 identified shadow IT instances, 25 resulted in a task reallocation. The participants attested a high quality. A management representative emphasized “the balance between flexibility, needed within the fast growing company environment, and efficiency.” To achieve a more robust evaluation we concluded with ADR in Company D.

<table>
<thead>
<tr>
<th>Shadow IT</th>
<th>IT service governance explanation</th>
<th>Specified task responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event management tool: Marketing sourced this cloud service. Data transfer from the enterprise system into the solution based on spreadsheets. The usage happened in a prototype stage with unclear requirements.</td>
<td>Management claimed for professionalism. Company C achieved this by embedding the solution in the IT service management and by adding testing and documentation. Thereby, the task execution stayed in the business due to acceptable risks, a mixed specificity, but a high uncertainty regarding requirements and future usage, and a small scope. Transparency facilitates possible future task transfers if uncertainty decreases.</td>
<td><img src="image" alt="Table 3. Shadow IT instance with remaining task allocation to the business" /></td>
</tr>
</tbody>
</table>

**Table 3. Shadow IT instance in Company C with remaining task allocation to the business**

**Setting of Expertise in Company D**

The ADR project in Company D enabled the final evaluation in an environment of expertise on governing shadow IT. In this German finance company, we analyzed Risk Management with 102 business-located IT solutions. These had previously been requested during audits. The project encompassed all constructs of task allocation (risk, specificity, scope, uncertainty). In total, 84 instances required task reallocation.

After discussion with participants, minor interventions were made. Revision was necessary when using the combined constructs for the task allocation. Overall, the experts emphasized the high quality of the procedure. An IT expert stated, “Business-located IT can constitute an asset; however, it also causes problems. Therefore, it is important to maintain transparency and define task responsibilities. This method increases our prior governance regulations.” A statement by a departmental head supports this: “The approach provides a good way to increase the quality of IT solutions implemented by business workgroups without reducing the advantages.” A representative from a business workgroup added: “The method is a good way to show necessary tasks and those currently missing. Besides creating this awareness, we welcome the allocation of tasks to the IT unit. However, we also affirm the importance of retaining particular service tasks in our group to ensure flexibility and usage of our specific knowledge.” Based on this positive evaluation, the company started to apply the approach to other departments and we could specify the reflection and learning from the BIE phase.

**Reflection and Learning**

This ADR stage moves conceptually from building an artifact for particular settings to applying that learning to a broader class of problems (Sein et al. 2011). While the initial design constituted less developed and detached constructs, the BIE process and learning from the participants led to refinement and combination of these. We now present the final design and the learning outcomes structured by the study’s research question: How should organizations allocate IT task responsibilities for identified shadow IT instances between a business workgroup and the IT unit?

A reasonable allocation follows risk- and TCE-related principles as shown in Figure 2. The decision of who is in charge leads to IT service governance forming a co-operation of business and IT units with shared tasks (Powell 1990). As a precondition, the structuring of components and subtasks (Picot 1990), including missing tasks, for identified shadow IT instances is necessary. Furthermore, sufficient IT
knowledge in business workgroups is essential if IT task responsibilities are to be allocated to them. A further procedure determines the task allocation between the business workgroup and the IT unit.

![Figure 2. Allocating task responsibilities for identified shadow IT.](image)

Initially, in cases of high risk, tasks are allocated to the IT unit to ensure a high level of control. This relates to the internal system risks that shadow IT and workarounds present to company goals, security, and compliance (Alter 2014; Haag and Eckhardt 2014; Zimmermann et al. 2014). Transfer to the IT unit and even re-engineering is reasonable, if highly relevant and critical shadow IT is of low quality, or the business workgroup has insufficient IT knowledge to maintain it. In the case of a task transfer, the IT unit delivers the newly allocated tasks or components based on the requirements of the business.

The TCE considerations of the exchange relationship between the business workgroups and the IT units provide another criteria to allocate tasks and address inefficiencies (Jones et al. 2004; Zimmermann and Rentrop 2014). In cases with acceptable risk, the specificity of IT tasks is at first decisive. An assignment of non-specific tasks or components to the IT unit will happen, because they are suitable for several solutions or because already existent resources can be reused. The transaction costs for such assignments are low. Specific tasks tend to stay in the business workgroup owing to the related idiosyncratic business knowledge, the transfer of which would be too costly. In between lie tasks with a mixed specificity that need to be addressed with regard to uncertainty. In cases with low uncertainty, the transfer of tasks with a mixed specificity to the IT unit follows the same reasoning as that for non-specific tasks. This inverts for high uncertainty. Business workgroups may want to experiment with an idea that has uncertain requirements resulting from external, environmental influences. In this situation, a transfer of knowledge to the IT unit would cause too high transaction costs. Finally, the scope of use is an influencing factor. If a service has a broad scope, the business requires IT consultation to ensure efficient task execution and further risk reduction. IT units can offer support with questions of technology or procedure.

These principles allow for an efficient and adaptive IT service governance for transparent business-located IT (Williamson 2005) and address several shadow IT challenges. First, it uncovers missing or unprofessionally provided tasks and inadequate components. Second, risk mitigation occurs with the allocation of tasks with due regard to criticality and quality. Third, by building allocations on the specificity of IT tasks moderated by the uncertainty, organizations can raise efficiency, while they keep innovation potential and adaptability of a business-located IT. Including the scope of use in this process supports a proper task execution due to the IT unit’s consultation function.

By building on research regarding managing shadow IT (Beimborn and Palitza 2013; Chua et al. 2014; Fürstenau and Rothe 2014; Zimmermann et al. 2014) and adding the perspective of allocating task responsibilities, these results contribute to the research on related IT governance questions (Györy et al. 2012; Winkler and Brown 2014; Zimmermann and Rentrop 2014). The artifact from the ADR process provides a way of achieving controlled, value-added IT services with defined responsibilities within the business workgroups. The procedure extents the current and potential business roles for delivering IT. It also provides a basis to proceed with questions of the control of business-located IT within an organization’s IT architecture (Fürstenau and Rothe 2014). Finally, it increases business awareness regarding shadow IT, which may lead to better coordination within organizations for future IT needs.
Conclusion

To address the problems of identified shadow IT instances, this study proposes principles for sharing IT task responsibilities between a business workgroup and an IT unit. Based on four ADR projects the results show generalized outcomes. Companies should transfer certain tasks to the IT unit, but for others, it is more beneficial to keep these within the business workgroup. This allocation can be based on risk and TCE dimensions and leads to an IT service governance of co-operation. Summarized, an acceptable risk level, highly business-specific tasks, and uncertainty justify the keeping of single tasks within the business workgroups, if IT resources and expertise are available, whereas others need to be transferred to the IT unit. The possibility of significant use with a large scope always makes it necessary to consult the IT unit.

Decision-makers may use these results to handle shadow IT in practice. When shadow IT becomes controlled, risks decrease and efficiency increases. Simultaneously, organizations maintain the adaptability of business-located IT. Practical implications are confirmed by the observed effects and the application of ADR companies themselves to other business processes.

Regarding theoretical implications, this study contributes to the governance of execution rights for IT services. It pursues research on application governance. Allocating task responsibilities at an IT service level between business and IT units may be adapted for formal IT when additional factors are considered. The results contribute to the literature on workarounds and EUC, regarding the control of these systems.

Some limitations exist to this study. We address the control of shadow IT at an initial, general level of task sharing. More research is necessary to specify the different applied constructs in detail, e.g., how risks can be categorized for task-sharing decisions, what dimensions exist of the scope of use, and what expertise in the business is required at the least. Furthermore, it is necessary to identify other factors that may be relevant, such as supporting technical solutions and competence of the IT unit. This is also connected to the inclusion of external suppliers, e.g., for Software as a Service, and the role of the IT unit in a possible direct relation between vendors and business units. Governance processes, therefore, need to be able to adapt to changing conditions. Furthermore, they need to accommodate highly regulated industries and recognize the consequences of shadow IT in such businesses. Considering IT architecture management, questions appear regarding the integration and monitoring of business-located IT in larger networks. The companies used here only represent a sample of the underlying reality. By investigating other cases and additionally including cultural aspects, researchers may advance a long-term control of shadow IT.

REFERENCES


