Fürstenau, Daniel; Rothe, Hannes; Sandner, Matthias

Leaving the Shadow: A Configurational Approach to Explain Post-identification Outcomes of Shadow IT Systems

Business & Information Systems Engineering

Bus Inf Syst Eng 63(2):97–111 (2021)
https://doi.org/10.1007/s12599-020-00635-2

RESEARCH PAPER

Leaving the Shadow: A Configurational Approach to Explain Post-identification Outcomes of Shadow IT Systems

Daniel Fürstenau · Hannes Rothe · Matthias Sandner

Received: 11 May 2018 / Accepted: 14 February 2020 / Published online: 9 March 2020

Abstract With the advent of end-user and cloud computing, business users can implement information systems for work practices on their own – either from scratch or as extensions to existing systems. The resulting information systems, however, often remain hidden from managers and official IT units, and are therefore called "shadow IT systems". When a shadow IT system is identified, the organization has to decide on the future of this system. The study uses a configurational perspective to explain outcomes of shadow IT system identification, as well as the mechanisms and contextual conditions which bring them about. For this purpose, 27 profiles of shadow IT systems were compiled by conducting 35 interviews with respondents from different positions and industries. The analysis gives insight into six distinct context-mechanism-outcome configurations explaining four outcomes that occur after shadow IT system identification, namely phase-out, replacement, continuing as IT-managed system, and continuing as business-managed system. These results contribute to the shadow IT literature and, more broadly, IS architecture and governance streams of the IS literature. They inform IT managers when these weigh decision options for identified shadow IT systems given different contextual conditions.

Keywords Shadow IT · IT governance · Application governance · Configurational method

Accepted after three revisions by Jens Dibbern.

Electronic supplementary material The online version of this article (https://doi.org/10.1007/s12599-020-00635-2) contains supplementary material, which is available to authorized users.

D. Fürstenau (✉) · H. Rothe
Department of Information Systems, School of Business & Economics, Freie Universität Berlin, Garystr. 21, 14195 Berlin, Germany
e-mail: daniel.fuerstenau@fu-berlin.de

H. Rothe
e-mail: hannes.rothe@fu-berlin.de

D. Fürstenau
Einstein Center Digital Future, Wilhelmstraße 67, Berlin 10117, Germany

M. Sandner
Department of Information Systems, School of Business & Economics, Freie Universität Berlin, Garystr. 21, 14195 Berlin, Germany
e-mail: matthias.sandner@fu-berlin.de

1 Introduction

The literature on shadow IT has noted the importance of shadow IT systems for organizations as well as the challenges and opportunities they pose (Behrens 2009; Haag and Eckhardt 2017). A shadow IT system can be defined as a hidden software system or an extension to a system that is neither developed nor approved by an official IT department or senior management (Fuerstenau and Rothe 2014). Its hidden character extends to a lack of awareness of the system in the organization, but also means that it was not part of IT planning (Kopper et al. 2018).

On the one hand, shadow IT can help to overcome deficits of central systems (Behrens 2009), to increase an organization's innovative power and speed of change (György et al. 2012; Fuerstenau and Rothe 2014), as well as to promote creativity and personal initiative. On the other hand, shadow IT can increase security risks (Silic and Back 2014; Walterbusch et al. 2017), deteriorate a company's architectural quality (Fuerstenau and Rothe 2014),

introduce redundancies and higher costs (Kopper 2017), as well as undermine control possibilities for IT management (Zimmermann et al. 2014) and violate companies' compliance rules (Panko 2006; Gozman and Willcocks 2015). In the face of power dynamics (Furstenau et al. 2017), interdepartmental conflicts (Walton and Dutton 1969), and political games (Behrens 2009), effective and functional governance plays a particularly important role in shadow IT (Winkler and Brown 2014; Zimmermann et al. 2016). Given the contradictory advantages and disadvantages of shadow IT, discussions on its management have come to the fore in recent years (Kopper et al. 2018).

However, the previous literature on shadow IT has largely taken the hidden character of shadow IT systems for granted without sufficiently acknowledging that shadow IT systems may start in a kind of "under-the-radar" mode while later on a shadow IT system can become known to more and more stakeholders which provides opportunities to reorganize the governance of the system. Furthermore, the literature has commonly implied that shadow IT systems are always to be brought to IT unit governance or be replaced by a new IT-governed system after identification and has ignored the possibility of alternative outcomes. Moreover, the literature lacks insight into the different paths that shadow IT systems can take after they have been identified and the underlying reasons for the differences.

The purpose of this paper is to *reveal the outcomes after the identification of a shadow IT system and to give insight into the mechanisms and contextual conditions which influence these outcomes*. This is important because shadow IT systems present veritable sources of organizational innovation that should be better exploited than in the past (Behrens 2009; Köffer et al. 2015). In addition, knowledge of possible and frequent outcomes is a prerequisite for establishing processes for controlling them (Zimmermann et al. 2014, 2017). The management and control of shadow IT systems is hardly possible without a grounded understanding of the forces that make some outcomes more likely.

We analyzed profiles of 27 shadow IT systems extracted from interviews with 35 shadow IT experts. Based on coding the data and using a configurational perspective (cf. El Sawy et al. 2010; Henfridsson and Bygstad 2013), we could identify four outcomes occurring after a shadow IT system was identified: phase-out, replacement, continuing as IT-managed system, and continuing as business-managed system. We were able to identify six configurations of contextual conditions, mechanisms, and outcomes. In a nutshell, the analysis shows the importance of social and technical deficiency mechanisms that jointly determine which shadow IT systems are not continued but phased-out or replaced. We also shed light on the role of contextual conditions for discerning IT and business management such as scope of use, task relevance, strict IT policies, and business-IT trust. Taken together, our study shows that there is much greater variation in post-identification outcomes, and it provides a configurational theory for why different outcomes are realized. Such configurational understanding is important where business-managed systems become more prevalent and the management of these systems becomes more shared among various stakeholders.

2 Research Framework

To develop our research framework, we first review different outcomes after shadow IT systems are identified. Based thereupon, we introduce a configurational perspective as a framework to capture which combinations of contextual conditions and mechanisms lead to these outcomes. Such a configurational approach is appropriate as multiple configurations of contextual conditions and mechanisms may contingently cause an outcome. Then, we tap into the different contextual conditions and mechanisms in detail. Finally, we summarize key outcomes, contextual conditions, and mechanisms of our study.

2.1 Shadow IT Post-identification Outcomes

In this paper, we focus on shadow IT systems that are hidden and later become identified. Haag and Eckhardt (2017) have used the notion of "covertness" to describe this hidden character. The term "covert" (versus "overt") is to be understood as the degree to which key stakeholders such as IT managers, line managers, or senior managers are aware of a system and the degree to which it is included in IT management processes (Kopper et al. 2018). Among these processes are IT risk and security management, IT portfolio management, IT service management, as well as enterprise architecture management. Multiple occasions can unmask a shadow IT system. Often these occasions are related to an organizational restructuring, a major IT transformation, or shortcomings in the system itself that lead to dysfunctions in business activities and make involvement of the IT unit necessary. However, the post-identification outcomes and the contextual conditions and mechanisms leading to these outcomes have so far received little attention in the literature on shadow IT.

In the broader literature on information systems, Recker (2016) identifies three generic strategies around information systems that are relevant for our investigation and present a valuable starting point to conceptualize post-identification outcomes.

Phase-out refers to a situation in which an information system is discontinued without a replacement system. Such a situation of ceasing an existing information system may occur when a system no longer contributes to

organizational aims (Rezazade Mehrizi et al. 2019). This could be due to a lack of functionalities or ended vendor support (Furneaux and Wade 2011). It could also be due to a reorganization that makes the supported work task obsolete or a displacement of people in an organization. Discontinuance has mostly been discussed in the context of organizational legacy systems (Rezazade Mehrizi et al. 2019; Furneaux and Wade 2011). It has, however, also been noted that shadow systems can be designed as temporary work systems that cease to exist after some service or product has been produced (Alter 2014).

Replacement refers to a situation in which a shadow IT system is discontinued after identification with another system replacing it. In this situation, users switch from one system to another one (Bhattacherjee et al. 2018; Polites and Karahanna 2012). As we are interested in outcomes after shadow IT identification, the former system is a shadow IT system and the latter system is possibly a new system operated by the official IT units.

The third generic strategy is continuance (Recker 2016). Continuance refers to a situation in which the same information system is further used for the same task, which should be specified in the context of our investigation by the way in which a system is governed after identification.

Drawing on the literature on application governance (Winkler and Brown 2013), Kopper et al. (2018) have distinguished two forms in which overt information systems can be governed. These forms refer to the extent by which the *task responsibilities* for a system remain in the business unit that created the shadow IT system or if they are taken over by the IT unit.

Continuing as IT-managed system describes a situation in which a shadow IT system remains operational but the main locus of control is transferred to the IT unit after the identification of the system. This means that the shadow IT system becomes an officially "IT-managed system" since the most important tasks related to the system are relocated to an IT unit (Kopper et al. 2018; Zimmermann et al. 2016).

Continuing as business-managed system refers to a situation in which a shadow IT system is continued after its identification and the business unit where it originated keeps the responsibility for it. As Kopper et al. (2018) note, such a system is more appropriately called a "business-managed system," as its covert character is morphed into an overt one. From a governance point of view, "business-managed" means that the system is managed in the business unit in alignment with the IT unit or in a split-responsibility model. Some reengineering may be necessary to comply with the company's IT policies. Figure 1 summarizes the four described outcomes and underlying decisions with respect to these outcomes.

2.2 Configurational Perspective

Understanding the complex causal influences that lead to different outcomes after shadow IT system identification requires a conceptual perspective that is powerful enough to account for equifinality. Equifinality refers to a situation where a system can reach the same outcome from different initial conditions and by a variety of different paths (Fiss 2007). A *configurational perspective* offers such a framework. It was introduced more broadly to the information systems field by El Sawy et al. (2010), and used by scholars such as Henfridsson and Bygstad (2013), Henningsson and Kettinger (2016), and Park et al. (2017). Such a perspective is particularly well suited to offer holistic and systemic explanations for phenomena. One of the logistical advantages of configurational methods is their ability to handle a medium number of cases, which would still be too many for individual case comparisons (Ragin 2014). Furthermore, a configurational perspective can account for

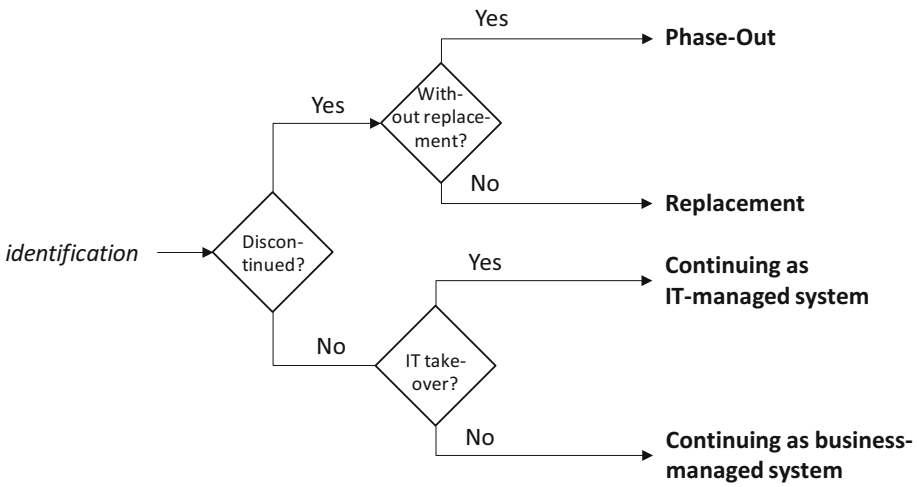

Fig. 1 Four post-identification outcomes for shadow IT systems

situations in which no single condition can produce an outcome but only the joint occurrence of multiple conditions. The configurational perspective offers a vocabulary to reason about these situations holistically using the concepts of *mechanism*, *context*, *outcome*, and *context-mechanism-outcome configuration* (Pawson and Tilly 1997).

A *mechanism* is a causally relevant process that produces an outcome (Bygstad et al. 2016). In the absence of the mechanism, the outcome will not occur. However, it may be the case that a causal mechanism only unfolds its driving force when it is combined with other mechanisms or conditions. In this situation, a mechanism may be necessary but is not sufficient for the outcome. As Henningsson and Kettinger (2016), we are interested in *deficiency mechanisms* that can be actualized or not. In the context of our study, we refer to a deficiency as *a low-quality feature of a system impacting future development possibilities*. Accordingly, if a deficiency cannot be resolved, it can become a deficiency mechanism causally driving the discontinuance of a shadow IT system.

The *context* presents further conditions for an outcome to occur. Conditions can be absent or present and thereby provide the environment to observe an outcome. In configurational analysis, there is no presumption about the level at which contextual conditions are located. In the context of our analysis, contextual conditions particularly describe the organizational setup in which processes take place that lead to discontinuing or continuing a shadow IT system.

Outcomes are the consequences of interest for a configurational analysis. They are produced through the interplay of mechanisms and contextual conditions. In this paper, outcomes of interest refer to the observable consequences after a shadow IT system is identified, namely phase-out, replacement, continuance as IT-managed and business-managed system.

Taken together, combinations of context-mechanisms-outcome are called *configurations*. A configuration describes a set of actualized or non-actualized conditions and mechanisms causing an outcome to occur (El Sawy et al. 2010). Such configurations present causal hypotheses, which describe when an outcome is to occur. The result of a configurational analysis is to be understood as a preliminary conjecture to be supported or refuted by data.

2.3 Contextual Conditions

In this section, we introduce different contextual conditions that contingently entail shadow IT system post-identification outcomes.

Scope of Use Scope of use refers to *the breadth with which a system is used throughout an organization* (Winkler and Brown 2013). Systems with larger scope may be distributed across many users, departments, and locations. They are used in many potentially critical routines. Different departments using a system can block each other and make changes more difficult. Thus, a larger scope may produce "gridlocks from an interplay of structural and behavioral complexity" (Agarwal and Tiwana 2015, p. 474). It is also plausible to suspect that systems with a larger scope of use are more deeply technically and organizationally embedded (cf. Winkler and Benlian 2012). A deeper technical embedding, in turn, implies that the systems are more difficult to discontinue, because many dependencies to other systems must be considered (Furneaux and Wade 2010, 2011). Furthermore, (dis-)investment decisions for more embedded systems are likely to have an impact not only at departmental level but also at wider organizational levels (Xue et al. 2008), making it harder to reach a decision. A larger scope of use could therefore represent a context in which identified shadow IT systems rather tend to be continued than discontinued.

Task Relevance We refer to task relevance as *the extent to which a task supported by a system has a critical impact on the organization* (cf. Morris and Venkatesh 2010). If a task is not relevant, it is likely to be an obsolete activity that is no longer important for an organization. Therefore, it is suspected that an information system supporting this task will also be suspended (Recker 2016). In contrast, shadow IT systems that support critical organizational tasks may not be abandoned (Zimmermann et al. 2016). Instead, such systems may be replaced by an IT-managed system or reengineered if they are deficient (i.e., of low quality) (ibid.). Therefore, task relevance represents an important contextual condition that signals the demand of the organization to support the task using an information system.

Strict IT Policies By IT policies, we refer to the standards, rules, and guidelines for the use and security of IT. Such rules can be *either strict or relaxed with regard to the development and use of shadow IT systems* (Haag and Eckhardt 2017). Relaxed IT policies represent a context in which the unauthorized procurement and usage of shadow IT systems is likely because low levels of restrictions exist (Lüker et al. 2016). A setting with strict IT policies has high levels of restrictions in place and in turn discourages the usage of shadow IT systems (Haag and Eckhardt 2017). IT policies may be an important context for shadow IT post-identification outcomes, because organizations with stricter policies may prefer to recentralize shadow IT systems after identification. In contrast, "laissez faire" organizations unofficially acknowledge policy-breaking as necessary (Martin et al. 2013), and find business-managed systems more acceptable (Gregory et al. 2018). Stricter policies may also signify an already powerful IT

department, which likes to extend its resource base by centralizing previously decentral IT systems (George and King 1991).

Business-IT Trust As another important contextual condition, we consider the level of trust between business and IT units. By business-IT trust, we refer to *mutual respect between both parties (business and IT) who interact openly, benevolent, non-opportunistically and value each other's abilities* (Mayer et al. 1995; Rousseau et al. 1998). In contrast, a distrustful relationship is characterized by opportunistic action that does not follow joint interest. Trust is an important dimension of the partnership between business and IT (Luftman 2003) and its social capital component (Schlosser et al. 2015). A trust relationship between business and IT units is likely to reduce the overall amount of shadow IT systems, because less subversive and hidden action is commensurate (Furstenau et al. 2017). A trust relationship can be a prerequisite for cooperation that enables its centralization (Wilkin and Chenhall 2010; Nwankpa and Roumani 2014). It is thus a necessary condition for a business to hand over the responsibility for a cherished system to an IT unit. We suspect trust between business and IT units plays a role in post-identification outcomes of shadow IT systems.

2.4 Deficiency Mechanisms

In this section, we introduce two deficiency mechanisms related to shadow IT post-identification outcomes: technical and social deficiencies. These mechanisms build on the socio-technical nature of change in information systems (Lyytinen and Newman 2008) and shadow IT systems as well as on the logic of deficiency mechanisms as conceptualized in this paper as drivers of discontinuation decisions.

Technological Deficiency Mechanism The first deficiency mechanism we introduce is related to the technology dimension of a shadow IT system. The technological deficiency mechanism refers to *structural issues arising from an insufficient technological basis (system architecture) or a lack of integration of the system in the overall system landscape*. There are several reasons for this, which can accumulate over time. First, a system could be built on a very narrow or simply outdated technical basis (e.g., server technology, operating system, database, code library, or middleware). This may decrease an organization's intention to further develop or maintain a system (Furneaux and Wade 2011). Alternatively, the system could hit a technological cliff when certain technological components need upgrades. For example, a system's technical basis may no longer be updated by the vendor and self-development may be too costly. Further technological challenges can relate to non-performant or complex integration (Huber et al. 2018). For example, uploading data to other systems may be too complex and a simple fix may not be in sight. When an insufficient access to official systems is circumvented by greatly expanding the IT landscape complexity, integration issues become more prevalent over time (Fuerstenau and Rothe 2014; Koutsikouri et al. 2018). Taken together, these examples show how technological problems and dependencies over time can create pressure that may lead to a negative outcome related to an identified shadow IT system.

Social Deficiency Mechanism A second group of deficiencies refers to the social dimension of a shadow IT system. It is defined as *structural issues with the actors involved in deploying or managing a shadow IT system or the tasks the system is applied to*. Key actors include employees and vendors as well as practices to mediate between people such as system documentation and communication. A deficiency mechanism related to key persons can arise in the moment when a system becomes dependent on a few people that later leave the company (Behrens 2009). This may happen when a key developer of a self-developed system retires, while the entire process chains have been built around the local system. Adequate documentation may not be available. However, even clear and comprehensible documentation can only partially compensate for the loss of key persons. Another set of issues in the people-related realm arises with vendors, which can become an important source of dependency and lock-in (Greenstein 1997), and finally pose a threat for the survival of a shadow IT system. First, there may be agency problems as when the vendor or consultant has an incentive to delay a project to justify additional payments. Secondly, a vendor might disappear before the end of the lifecycle of the shadow IT system is reached; therefore, the further development is not guaranteed. Furthermore, a vendor can cease support for a product, as observed frequently with self-developed systems depending on Excel/Visual Basic (cf. Raden 2005). Altogether, social issues may form a deficiency mechanism that increases dependencies between individuals within and across organizational boundaries.

Another problem in the social realm relates to the business tasks associated with a shadow IT system (cf. Aral and Weill 2007). It includes a system's ability to correctly apply a business logic (Markus 1983). Faulty business logic hidden in spreadsheet applications can be hard to decipher in the progress of further development and at some point led to poor decisions (Raden 2005). A system should solve a task with appropriate quality, be usable by the people entrusted with the task, and be expandable with regard to the underlying data and functional structure if the task requirements change (Panko 2006; Tarafdar et al.

Table 1 Research framework for configurational analysis

Grouping	Concept	Definition	Possible values	Key references
Contextual conditions	Scope of use	The breadth with which a system is used throughout the organization	0 – Small scope 1 – Large scope	Winkler and Brown (2013), Xue et al. (2008)
	Task relevance	The level of criticality of the task supported by the system for the organization	0 – Not relevant 1 – Relevant	Recker (2014), Zimmermann et al. (2016)
	Strict IT policies	Level of IT policy enactment with regards to consumer IT devices and shadow IT	0 – Relaxed 1 – Strict	Haag and Eckhardt (2017), Lüker et al. (2016)
	Business-IT trust	Level of partnership between business and IT regarding an open, benevolent, and mutually respectful relationship	0 – Not trustful 1 – Trustful	Luftman (2003), Furstenau et al. (2017)
Deficiency mechanisms	Technical deficiency	Structural issues with low quality of the technological base or integrations of a system	0 – Not actualized 1 – Actualized	Furneaux and Wade (2011), Huber et al. (2018)
	Social deficiency	Structural issues with low quality of skills of actors involved in, practices managing, or with the character of the tasks a system is applied to	0 – Not actualized 1 – Actualized	Aral and Weill (2007), Zimmermann et al. (2016)
Outcome	Phase-out	System is discontinued without replacement system	0 – No phase-out 1 – Phase-out	Recker (2016), Furneaux and Wade (2011)
	Replacement	System is discontinued and users switch to a replacement system	0 – No replacement 1 – replacement	Recker (2016), Rezazade Mehrizi et al. (2019)
	Continuing as IT-managed system	System is continued and taken over by IT unit	0 – Not IT-managed 1 – IT-managed	Winkler and Brown (2014), Kopper et al. (2018)
	Continuing as business-managed system	System is continued and handled as business-managed system	0 – Not business-managed 1 – Business-managed	Kopper et al. (2018)

2015). In addition, the quality of the processes and support structures surrounding a system can also be important (Zimmermann et al. 2016). If such structures do not exist, users can be disappointed and turn away from the system. Taken together, task-related social deficiencies imply that a system is currently or in future not in a position to fulfill the needs associated to the tasks of its core audiences.

2.5 Summary

Table 1 summarizes contextual conditions, mechanisms, and outcomes, representing the research framework for our configurational analysis.

3 Methods

3.1 Data Collection

The literature on shadow IT post-identification outcomes is sparse and consists mostly of narrative accounts (Behrens 2009; György et al. 2012; Silic and Back 2014; Kopper and Westner 2016). Because the cases in the literature often do not provide the richness needed for a literature-based qualitative comparative study (Henfridsson and Bygstad 2013; Henningsson and Kettinger 2016) and because we wanted to derive empirically grounded causal hypotheses for shadow IT post-identification outcomes, we conducted interviews with experts. The interviews helped to get a broad overview from respondents in different industries and positions related to shadow IT systems. Following Meuser and Nagel (2009), we use the term "expert" here in a broad sense indicating that a person is knowledgeable related to the subject area as a specific field of action.

We conducted 35 interviews with 29 participants in two rounds. Interviews were appropriate for this study for three reasons. First, the interviews allowed consolidating diverse terminologies from different persons without degrading the potential richness of meaning (Alvesson 2003). Second, the interviews were relatively efficient to explore a broad spectrum of systems, functions, industries, and roles without being bound to the idiosyncrasies of one setting. Third, the responses enabled us to collect the essence of a system's identification outcomes and its reasons into one or a few interviews while maintaining the ability to reflect on and inquire new factors.

Table 2 Data sources

System	#Int.	Interviewees	Co.	Industry	Size	Country
S_1 BOARD	3(*)	IT manager (P_1), CIO (P_2), IT developer (P_3)	A	Utilities	7500	DE
S_2 CRM	2(*)	Developer (P_4), outsour-cing partner (P_5)	B	IT Services	100	DE
S_3 CONTRACT	1(*)	IT consultant (P_6)	C	Insurance	30,000	DE
S_4 CARGO	1(*)	Developer (P_7)	D	Transport	> 100,000	DE
S_5 IT DB	1	IT consultant (P_8)	E	IT Services	3000	DE
S_6 MARKET DATA	3	Project manager (P_9), IT architect (P_{10}), IT security (P_{11})	F	Banking	4000	DE
S_7 ALGO	2	Developer (2x) (P_{12}, P_{13})	F	Banking	4000	DE
S_8 FIXINGS	1	Developer (P_{14})	F	Banking	4000	DE
S_9 HOT BILLING	1(*)	Business manager (P_{15})	G	Telco	> 100,000	DE
S_{10} BILL-SWEEP	1(*)	Business manager (P_{15})	G	Telco	> 100,000	DE
S_{11} IP-TEL	1(*)	Business manager (P_{15})	G	Telco	> 100,000	DE
S_{12} BOOKING	1	Internal consultant (P_{16})	H	Transport	> 100,000	DE
S_{13} ASSET MGMT.	1	IT consultant (P_{17})	I	Production	5000	DE
S_{14} CUST. MGMT.	1(*)	IT consultant (P_{18})	J	Banking	40,000	DE
S_{15} EQUIP	1(*)	IT consultant (P_{19})	K	Technology	> 100,000	DE
S_{16} ADMIN	1	IT manager (P_{20})	L	Public Sector	750	DE
S_{17} AERO	2(*)	IT consultant (2) (P_{19}, P_{21})	K	Technology	> 100,000	DE
S_{18} FIN-CALC	1	Business manager (P_{22})	M	Banking	750	DE
S_{19} RECON	1	IT manager (P_{23})	M	Banking	90,000	DE
S_{20} DOC-2-DOC	1	IT consultant (P_{24})	N	Healthcare	16,000	DE
S_{21} FILE	1	IT manager (P_{25})	O	Technology	> 100,000	CH
S_{22} SETTLE	1	Architect (P_{26})	P	Insurance	14,000	DE
S_{23} UNDERWRITE	1	Architect (P_{26})	P	Insurance	14,000	DE
S_{24} SIM DISASTER	1	Architect (P_{26})	P	Insurance	14,000	DE
S_{25} PDM	1(*)	IT consultant (P_{27})	Q	Production	1000	DE
S_{26} MUNICIPAL	1(*)	Business user (P_{28})	A	Utilities	7500	DE
S_{27} CTRL COCKPIT	2(*)	Business user (P_{29}), IT manager (P_1)	A	Utilities	7500	DE
Total	35		17		100– > 100,000	

In brackets (*): follow-up interview conducted

#Int… number of conducted interviews, Co… company assignment

We first created a contact database ($N = 118$) from our own industry experience and public sources and then contacted potential interviewees. The contacts that agreed to participate in our interviews ($N = 35$) came from diverse industries and represented different roles. These included business roles such as creators/developers, sponsors, and users of shadow IT systems as well as IT management roles such as IT managers, architects, security and governance representatives, plus consultants being concerned with the control, migration, or discontinuance of shadow IT systems. Table 2 summarizes our data sources.

The investigated systems stemmed from a diverse set of organizations, whereby all organizations in question were headquartered in Germany or Switzerland. Their size ranged mostly from medium to large. Per default, we designed our study so that one respondent told the story of one shadow IT system case. Following the same interview pattern, in six of the cases we could consult with multiple respondents to back-up and triangulate the individual case. We made sure that all interviewees had direct access to the shadow IT system in scope to foster the credibility of their statements (Madill et al. 2000). We confirmed this by asking respondents for specific examples and events indicating their involvement in the process of developing, using, or overseeing the shadow IT system.

The interviews took place in a period between January 2015 and October 2016.[1] They generally lasted between 45 min and 1 h and were performed either face-to-face, via telephone, or via audio–video conferencing tools. We recorded the interviews where the interviewee agreed with

[1] Four additional interviews came from an earlier empirical study that was conducted in 2012 in the waste management industry. These interviews were included because they provided rich background information on two of the shadow IT systems of the present study.

the procedure (75% of the interviews). These interviews were transcribed. For the other interviews, we produced field notes within 48 h after the interview substituting for the transcription. We asked interviewees for a follow-up as well as for additional materials on the discussed system. Whereas we obtained rich materials such as documentations and vendor presentations for some shadow IT systems, in most cases no written documentation was available. If available, the materials informed our analysis and helped to triangulate our results.

Against a critical realist epistemology (Bygstad et al. 2016) our interviews followed a narrative strategy that considered concrete stories and the interviewee's personal experiences (Clandinin and Rosiek 2007). We did so by focusing on specific cases that the interviewees perceived as "critical" or "revelatory," because we expected to learn most from reflecting on these cases. We had prepared an interview guide that tapped into three main areas: (1.) The "story" of one specific shadow IT system, the critical challenges therein, and changes in the system's operations and/or governance, and (2.) more general observations drawing on the interviewees broader experience with the topic area and further cases. In addition, we (3.) asked for descriptive facts (the interviewee's industry experience, the interviewee's current position and role, and descriptive information regarding the shadow IT system). We treated the resulting data as "fixed," seeking to identify patterns in the data that would be independent of the specific context (Clandinin and Rosiek 2007).

3.2 Case Database, Coding, and Configurational Analysis

Our case analysis consisted of multiple rounds and iterations. In a first round of summarizing and coding, we created a detailed case tableau in which we described every identified shadow IT system using one column. As some interviewees provided rich accounts of multiple shadow IT systems, while others did not provide sufficient information on specific systems, the number of cases does not match the number of interviewees.[2] Our case tableau included data such as a short description (ca. 50–100 words; see Appendix 1, available online via http://link.springer.com), background facts, reasons for the origination of the system, growth patterns, incidents (challenges), observed outcomes, and other context factors. In this first round, a coding of incidents took place by author 1 and 3 using a code set abductively derived from the literature and emerging empirical insights. This means that inductively emerging codes in the empirical material where tied back to theoretical concepts from the literature, which were then reapplied to the empirical material in an iterative fashion. The coding followed a "consensus principle" to guarantee agreement among coders (Harry et al. 2005, p. 6).

Based thereupon, this paper uses a *configurational perspective* (cf. El Sawy et al. 2010; Henfridsson and Bygstad 2013) to elucidate outcomes of shadow IT system identification and underlying reasons. As applied here, our configurational analysis distinguishes explanatory factors into mechanisms and contextual conditions. We aggregated previously derived codes for incidents into two deficiency mechanisms (social and technical) and recoded the cases for the presence or absence of the theorized contextual conditions. A table was prepared that helped in comparing similarities and differences across cases (see Appendix 2), which was further condensed and abstracted from to derive the results presented in the next sections.

4 Configurational Analysis

Our configurational approach identified six configurations (1–6) that are associated with either of the four possible post-identification outcomes of phase-out, replacement, continuing as IT-managed system, and continuing as business-managed system. Figure 2 displays the results.

4.1 Phase-Out

We refer to a *phase-out* as a situation in which *an identified shadow IT system was discontinued after its identification without putting a new system in place*. Three systems in our sample matched the outcome combination of phase-out, associated with one combination of conditions.

Configuration 1: Phasing-Out the Insignificant There was one coherent context-mechanism-outcome configuration for phase-out (3 cases), as well as one configuration that was dropped because it had only limited support in our data (1 case). For all cases, social and technical deficiencies were actualized. At the same time, the contextual conditions were identical. Phase-out occurred in a context in which the system was small in scope, where a distrustful relationship existed, relaxed IT policies were in place, and the task was not particularly relevant to the organization. The unconfirmed configuration differed in the contextual conditions with strict IT policies in place.

One example was a board computer system in a recycling firm (S_1). The system supported the routing of trucks using GPS data. It was introduced in one of the firm's main subsidiaries. Neither was a central system available nor had the IT department the resources and showed the will to develop a new system. The subsidiary hired a consultant

[2] Respondent data which could not be assigned to specific cases was used in the discussion only.

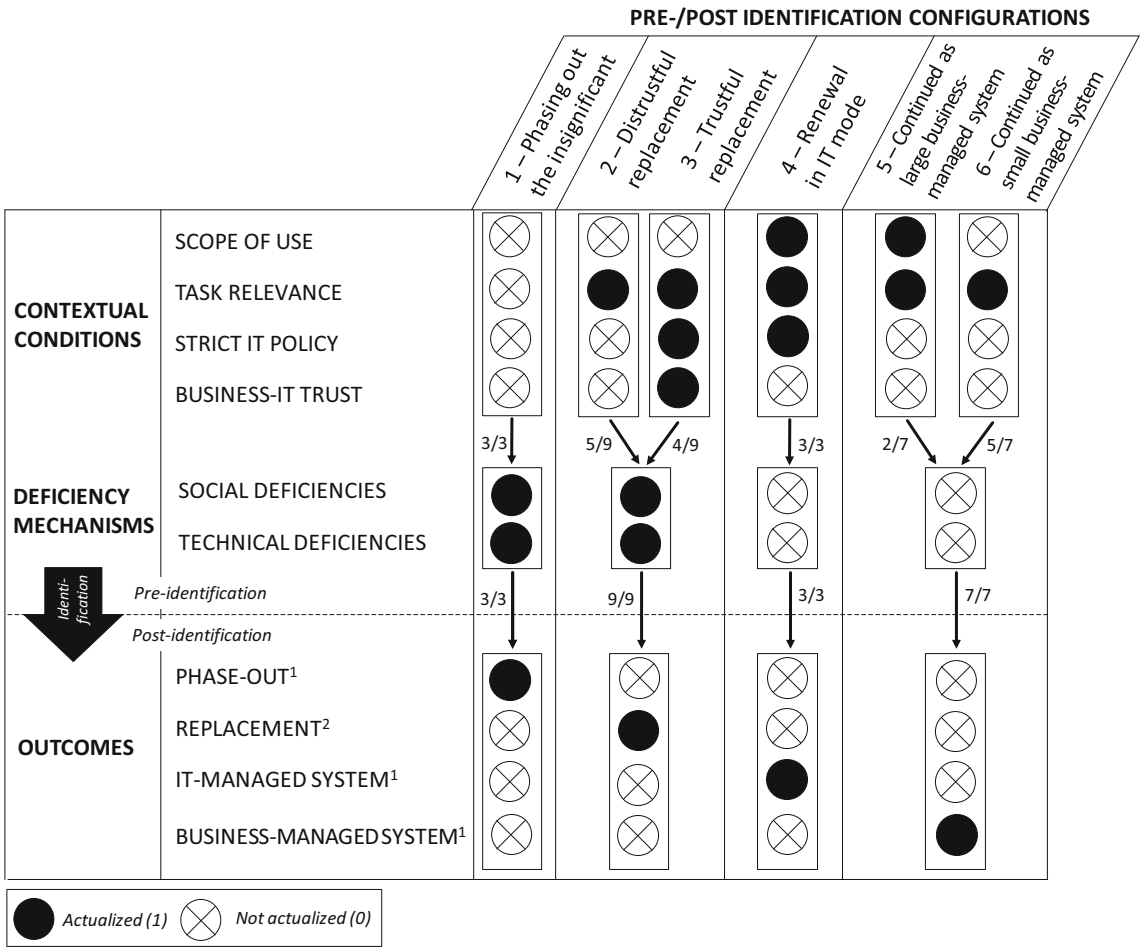

Fig. 2 Configurations of shadow IT systems pre-/post-identification. [1,2]Number of excluded system per outcome due to requirement of at least two identical cases per context-mechanism-outcome configuration (compare with Ragin 2014)

who in turn was affiliated with a software development company. However, various technical and social deficits came to light. The technical platform (Windows CE) on which the system relied had limited capacities and was quickly outdated (*technical deficiencies actualized*). In addition, the consultant had set an initial price that was too low, which later turned out to be untenable. The contracted software development company went bankrupt and the system could not be implemented as planned (*social deficiencies actualized*). Therefore, it was mounting technical and social deficiencies that triggered discontinuance. This happened in a context characterized by a distrustful relationship between IT and the local subsidiary (*trust not actualized*). The IT unit considered only costs as important and was not responsive. In consequence, the local subsidiaries did not see them as a trustworthy business partner. Moreover, the IT unit had not set strict policies for preventing the external procurement (*relaxed IT policies*). When the IT department was later involved, it was too late and the system was already integrated into the trucks. A new system was not introduced at this stage because the task was not considered relevant enough (*task relevance not actualized*). Moreover, the system's small size in relation to a large-scale ERP project on the horizon (*small scope*) contributed to the decision to postpone investments into a new system until the new ERP was rolled out.

The other examples confirmed that significant risk combined with a non-critical task explain why some shadow IT systems are discontinued without (immediate) replacement.

4.2 Replacement

By replacement, we refer to the outcome of a discontinued shadow IT system post-identification with a new system replacing it. For 11 systems in our sample, replacement was the observed outcome. We found two configurations explaining this outcome combination: one configuration marked by distrust (5 cases) and another by business-IT trust (4 cases), as well as two more configurations that were dropped as each had only limited support (1 case each). The unconfirmed configurations differed in scope because

they were large, as well as social deficiencies that could not be observed in one case.

Configuration 2: Distrustful Replacement Similar to the phase-out, we observed replacement to occur in situations in which a small system faced social and technical deficiencies in a context that lacks trust between business and IT.

One example is an *underwriting system* in a reinsurance company (S_{23}). The system supported sales employees in closing reinsurance contracts, especially in the process of calculating damage ratios. When the company migrated to another Excel version, the system was replaced by a new system as part of a migration project. From a standpoint of technical deficiencies, especially performance issues and self-developed interfaces to a data warehouse/BI system turned out to be problematic (*technological deficiencies actualized*). At the same time, the system relied heavily on knowledge from externally contracted consultants, creating a critical dependency (*social deficiencies actualized*). Tensions between IT and business units revealed a lack of trust in the abilities of the IT unit. The IT unit was perceived as not being able to fulfil the units' demands in a satisfactory manner and the business unit turned to external consultants. This happened in a setting in which IT policies were not enacted (*relaxed IT policies*). The system's small scope made replacement for the necessary task feasible (*small scope*).

Other cases showed that a subversive business unit had procured a system that later proved unsustainable due to its social and technical deficiencies. Thus, the identification of the system presented an event that made the replacement of the system by a central one more likely. The identification led to a "hostile takeover" after which a distrustful relationship remained, if it was not further enforced.

Configuration 3: Trustful Replacement Another mechanism-context-outcome combination existed for replacement in which business-IT trust was present. A case example was an *IT management database* in an IT service management firm (S_5). The system, programmed by a hands-on IT person, helped to automate IT portfolio planning using a self-developed Access database. The system was discontinued due to problems arising from the inextensible, chaotic data structure and the single-person dependency, which contributed to serious planning failures or almost-failures using unreliable data from the system (*social and technological deficiencies actualized*). However, the decision to replace the shadow IT system by a new system was supported by the fact that the creator of the system was not demonized but involved in the implementation of a new system (*business-IT trust actualized*). Thus, the system creator could take ownership of the new system and was consequently willing to contribute his domain-specific knowledge.

Other cases confirmed that social and technical deficiencies contributed jointly to the decision to not continue the system, but that trust, and the involvement of main shadow IT owners, helped in creating a new system.

4.3 Continuing as IT-Managed System

By *continuing as IT-managed system*, we refer to a situation in which the responsibility for a shadow IT system is transferred to an IT unit after identification.

Configuration 4: Renewal in IT Mode This outcome was brought about by one context-mechanism-outcome combination (3 cases). The confirmed confi-guration was characterized by the absence of deficiency mechanisms and a context which was characterized by a large scope, a relevant task, strict IT policies and a distrustful business-IT relationship. A further configuration, differing in the presence of technical deficiencies, was dropped due to limited support in our data (1 case).

One example for renewal in IT mode is a market data management system in a mid-sized bank (S_6). The system automated the delivery of external market data to internal business units and thereby helped to be more competitive. After the system was identified in the context of a reorganization, it was decided to keep the system and to transfer the responsibility to the IT unit (*outcome: IT-managed system*). The absence of social and technical deficiencies – enabled by the "good performance" (Project manager, P_9) (*social and technological deficiencies not actualized*) of the project team who implemented the system – contributed to the decision to continue the system. The necessity of the system for the organization, indicated by its large user base (*large scope*), contributed to the decision to continue the system. The setting in which this happened was generally *distrustful* with a great distance between business and IT units (*business-IT trust not actualized*). This means that no close exchange took place between business and IT. Due to general risk considerations and a restricted policy of recentralization of decentralized systems (*strict IT policies*), it was decided to transfer the system to IT governance.

The other examples confirmed that a large scope contributed strongly to continuing a system in an IT-managed mode. This was because the systems had already obtained a critical status for the organization. Also, strict IT policies presented a fertile ground for continuing a system in an IT-managed way. Such policies favored choosing an IT relaunch over business continuance. Finally, it was the absence of major social and technological deficiencies

which let IT units consider an IT relaunch as a viable option.

4.4 Continued as Business-Managed System

We refer to *continuing as business-managed system* as a situation in which a shadow IT system is continued and the developing business unit keeps the control after the system's identification. The outcome was associated with two configurations, which differed only in the extent to which the continued system had a *large scope* (2 cases) or a *small scope* (5 cases). One configuration was dropped since it had only limited support in the data (1 case). The dropped configuration differed in the presence of observable technical deficiencies. Across confi-gurations, a powerful business unit maintained control post-identification against a relatively weak IT.

Configuration 5: Continuing as Large Business-Managed System One example for *continuing a large business-managed system* was a customer management system in a bank (S_{14}). The system stored marketing data "wickedly" (IT consultant, P_{18}). After the system was identified, it was continued and the business unit kept control over the system, although it was registered in the application portfolio management (*outcome: continuing as business-managed system*). The system was important for the business unit (*task relevance actualized*) and it worked as intended (*social and technological deficiencies not actualized)*. The system served the entire marketing unit, and several interfaces to other systems existed (*large scope*). Although the IT unit wanted to gain more control, there were limited information flows and the business unit did not want to make its requirements transparent (*business-IT trust not actualized*). The business unit blocked a change in governance and continued to develop the system with an external consultant. According to IT consultant P_{18}, the company's "relatively timid" IT procurement policies (*relaxed IT policies*) allowed business units to contract external IT service providers relatively freely.

Configuration 6: Continuing as Small Business-Managed System One example for this configuration was a disaster management simulation in a reinsurance firm (S_{24}). After the system was identified, it was continued in the business unit while being "on the radar" of the IT unit (*outcome: continuing a business-managed system*). The conditions under which the system evolved proved important for the chosen governance. Since the IT unit was relatively weak and lacked resources, the unit could not develop the necessary knowledge and capabilities to maintain the system. This inability was interpreted by the business unit as lacking ability and is indicative for a distrustful relationship (*business-IT trust not actualized*). Furthermore, the IT policies of the company did not force the system to be centralized (*relaxed IT policies*).

Overall, the examples confirmed that changes to the status quo were not desirable because distrust existed between business and IT unit, while social and technical challenges did not pose an immediate threat that would have justified discontinuance. Business rationales for continuing the systems as business-managed systems resulted from specialized needs for knowledge existing only in the business units. The trust-lacking relationship between business and IT and weak IT unit power made the transfer in the cases in turn less likely or excluded this option entirely.

5 Discussion

The paper aimed to reveal shadow IT post-identification outcomes and to give insight into the underlying reasons for when which outcome occurs. Taking a configurational perspective, we identified six distinct configurations of deficiency mechanisms under the presence of different contextual factors explaining four outcome combinations: phase-out, replacement, continuing as IT-managed system, and continuing as business-managed system.

In general, it could be seen that phase-out and replacement, representing outcomes in which the shadow IT system was discontinued post-identification, were brought about by a combination of social and technical deficiencies. Continuing as business-managed system represented another outcome, which was found in a constellation of distant, disengaged, or overloaded IT units that did not perceive urgency with regard to a functioning system. Finally, continuing as IT-managed system represented a special case of a committed IT unit – driven by strict IT policies or requirements – taking over control over a shadow IT system post-identification. In the following, the deficiency mechanisms and contextual factors are analyzed in detail.

5.1 Key Mechanisms and Contextual Conditions

One main insight of our study was the joint occurrence of *social and technical deficiencies* for discontinued systems. Illustrative for this finding was the Board Computer System (S_1) where architectural problems and a problematic vendor relationship coincided. While it may be possible to compensate for problems in one dimension by strong work in the other, problems in both dimensions made the investigated organizations act on the deficiency and discontinue the affected system. This finding is consistent with Lyytinen and Newman's (2008) conceptualization of change in information systems as a socio-technical process.

In this view, changes in one component of a system (e.g., a technological break-down caused by excess input) may at some point create a critical incident which, when combined with further deficiencies such as key people leaving, makes the problem pass a threshold where it can no longer be accepted. This can then trigger further responses such as the discontinuance of a system in order to re-establish the stability of the entire work system. Based thereupon, it can be reasoned that mounting social and technical problems occurring simultaneously can lead to discontinuance because the system poses too high risks or does not create enough value for the organization.

Secondly, *large scope* and *task relevance* proved to be important contextual conditions to understand post-identification outcomes. Large scope in many cases shows the embeddedness of a system, Embeddedness is defined as the extent to which a system is used in organizational processes or is technically connected to many other systems (Furneaux and Wade 2011). As Furneaux and Wade (2011) found, embeddedness of a system represents an important factor for discontinuance decisions. Usage in critical tasks or many interfaces to other systems can represent impeding factors creating continuance inertia. This is what our analysis showed. Out of eight large systems, only two were discontinued. One of the discontinued systems, a file-sharing service (FILE: S_{21}), was large in user base but low in technical complexity and embeddedness in routines, making the switch-over to a centralized system feasible. Another large system, a customer relationship management system (CRM: S_2) could be replaced, because employees had developed further Excel sheets complementing the newly implemented replacement system, thus making replacement less mentally and economically costly for them. Our finding is also in line with Swanson and Dan's (2005) observation that system size (*large scope*) is positively related to a system's remaining life expectancy.

Thirdly, we found that strict *IT policies* help to discern, as a contextual factor, between continuing a system in a business-managed versus IT-managed mode or discontinuing the system. In the configuration "renewal in IT mode," strict IT policies were observed together with continuing a system in an IT-managed mode. This was the case when the shadow IT system was generally of good quality and critical for the organization. A strict IT policy in such situation helped to enforce centralization. Another pathway indicated that strict enterprise IT policy may equally contribute to replacement. This was because strict policies went together with strict assessment procedures making those systems which could not be easily enhanced (e.g., implementing secure login) the target of replacement. This finding is generally in line with the literature on compliant use of IT (Panko 2006; Hoffmann et al. 2015; Lüker et al. 2016; Culnan 2019).

Finally, we found that *trust* between business and IT units is necessary to accept a replacement system for an identified shadow IT system. In configuration 3 (*trustful replacement*), this was the case because the shadow IT creators were directly involved or participated in developing or implementing a new system. Schlosser et al. (2015) have shown that social alignment between business and IT units can be fostered at the operational level by increasing the degree of social capital between an organization's business and IT units, IT personnel's business understanding, and a set of formal and informal IT governance mechanisms. We found that a trust-lacking business-IT relationship did in some constellations contribute to a business department's wish to maintain ownership (configuration 5 & 6). There were, however, also cases where a trust-lacking relationship and continuation as IT-managed system were observed together (configuration 4) due to risk and compliance considerations. Trust should be considered as an important contextual condition that deserves further attention.

5.2 Limitations

Before elaborating on theoretical implications, we will mention several limitations of our study. First, we have mostly relied on single respondents to reconstruct the profiles of the systems. Their role or relationship to the shadow IT system may affect their responses. We aimed at consulting multiple sources of evidence where possible, but future studies could equally involve each of these roles (user, sponsor, developer, and IT control) for each system to avoid potential biases. We were also not able to triangulate some of the information from interviewees with written documentation, because there was none available. Business units often intentionally cover the design and use of shadow IT systems. The lack of documentation is a direct result. Hence, this limitation might only be resolved through direct observation of development of such systems in the future. An additional limitation of the study is that it did not track the development of shadow IT systems over time. The understanding of the life cycle of shadow is limited to the perspective at one point of time (at which the interview was conducted). Furthermore, only such shadow IT systems could be considered which people were willing to talk about. No systematic scanning was considered feasible here. Moreover, we acknowledge the limited number of cases per configuration, which calls for collecting data on more cases. Finally, our focus on "systems" might have biased our view and future studies may devote similar attention to other artifacts such as cloud services, hardware devices, and technical tools (cf. Zainuddin 2012; Silic and Back 2014; Matt 2018).

5.3 Theoretical and Practical Implications

Our findings extend the shadow IT literature as well as the architecture/governance streams of the IS literature. While the existing literature has already considered challenges related to shadow IT systems (e.g., Raden 2005; Panko 2006; Behrens 2009; Fuerstenau and Rothe 2014; Haag and Eckhardt 2017; Haag et al. 2019), the literature lacks systematic analyzes of shadow IT post-identification outcomes, considering the underlying mechanisms and contextual conditions. We contribute to this literature by suggesting a configurational theory of shadow IT post-identification outcomes, which introduces deficiency mechanisms and contextual factors that explain these outcomes. Moreover, we regard our paper as a contribution to future efforts for increasing the controllability over a shadow IT system's lifecycle. As the identification of a shadow IT system can be followed by strong interventions such as discontinuing a system, knowledge about mechanisms and contextual factors may help to increase the manageability of shadow IT systems as well as their transfer from a "covert" to an "overt" mode in which they are managed openly with oversight of the IT unit (Zimmermann et al. 2016, 2017; Haag and Eckhardt 2017; Kopper et al. 2018).

For CIOs and IT managers it is important to be fully aware of the different options on how to proceed when a shadow IT system is identified. Our findings suggest that systematic assessment of contextual factors as well as social and technical deficiencies might offer good grounds for IT managers to decide. Considering these factors is increasingly important as demands on IT governance are gradually changing with digitalization (Urbach et al. 2019). Our research framework might inform standard procedures for handling identification events in three ways. First, it provides an overview of the different courses of action which effectively leads to a more founded decision making. Second, assessing social and technical deficiencies while incorporating knowledge on the contextual conditions provides a method to weigh potential risks against business opportunities for potentially innovative systems. Our configurational analysis implicates that low-quality systems which showed both social and technical deficiencies were regularly phased-out or replaced. For high-quality systems, in turn, governance changes from business-managed to IT-managed depended on the context, for instance whether strict IT policies were in place. Through IT policies and business-IT trust, companies can shape which identified shadow IT systems are transferred to or replaced by central IT systems profiting from valuable business insights. Third, transparency of how to handle shadow IT systems further legitimizes a decision and reduces unintended consequences. Particularly, weakly legitimized phase-out or (distrustful) replacement of a system might severely impact existing business practices and individual motivations of shadow IT system developers and users as well as (further) harm business-IT trust.

5.4 Future Research Opportunities

In addition to confirming or revising our findings by means of additional cases and conducting a large-scale study to test our configurational hypotheses, we see four particularly promising ways to proceed further. First, we took a comparatively static perspective as we focus on one particular point of time in the life-cycle of a shadow IT system, its identification and consequent outcomes. Future work could make more explicit the temporal dynamics and processes that link the identified mechanisms and other life cycle transitions. In relation to that point, one could delve deeper into particular cases and explore in more detail the industry and other contextual conditions beyond the ones analyzed in our study. Second, we found a trustful relationship between business units and IT units to be an important contextual condition. The outcome of a shadow IT system identification, however, has an impact on these relationships, for instance, the phase-out of a cherished system. The relationship between shadow IT systems and trust may leave room to find self-reinforcing mechanisms. Third, we considered governance-related outcomes after identification as a consequence of IT policies in place. Future work may also consider how a policy for using shadow IT system is issued after the identification. Forth, future work may aim at designing a theory-guided managerial governance framework that supports the allocation of task responsibilities for shadow IT systems between business and IT units.

6 Conclusion

Shadow IT systems today pose many challenges and opportunities for organizations that may become visible when such systems are identified by management or the official IT. We started our analysis from four theoretically derived outcomes of these identification events, namely phase-out, replacement, continuing as IT-managed system, or continuing as business-managed system. We found that technical and social deficiency mechanisms predominantly determine discontinuance. At the same time, the contextual conditions chiefly determine the chosen governance regime for continued systems. The exploration of context-mechanism-outcome configurations, thus, helps us to further understand the effects of pulling shadow IT systems out of the shadow. This research contributes to the shadow IT literature while building upon IS literature on IT

architecture and governance. The configurational approach informs IT managers on how to weigh decision options when identifying shadow IT systems.

Acknowledgements Open Access funding provided by Projekt DEAL. We thank the Senior Editor and the Associate Editor as well as the reviewers for their sustained guidance during the entire review process. For helpful inputs and comments, we also thank Dr. Dieter Masak and Dimitrios Anapliotis.

References

Agarwal R, Tiwana A (2015) Editorial – Evolvable systems: through the looking glass of IS. Inf Syst Res 26:473–479

Alter S (2014) Theory of workarounds. Commun Assoc Inf Syst 34:1041–1066

Alvesson M (2003) Beyond neopositivisits, romantics and localists: a reflective approach to interviews in organizational research. Acad Manag Rev 28:13–33

Aral S, Weill P (2007) IT Assets, organizational capabilities, and firm performance: how resource allocations and organizational differences explain performance variation. Organ Sci 18:763–780

Behrens S (2009) Shadow systems: the good, the bad and the ugly. Commun ACM 52:124–129

Bhattacherjee A, Davis CJ, Connolly AJ, Hikmet N (2018) User response to mandatory IT use: a coping theory perspective. Eur J Inf Syst 27:395–414

Bygstad B, Munkvold BE, Volkoff O (2016) Identifying generative mechanisms through affordances: a framework for critical realist data analysis. J Inf Technol 31:83–96

Clandinin DJ, Rosiek J (2007) Mapping a landscape of qualitative inquiry: borderline spaces and tensions. In: Clandinin DJ (ed) Handbook of narrative inquiry: mapping a methodology. Sage, Thousand Oaks, pp 35–76

Culnan MJ (2019) Policy to avoid a privacy disaster. J Assoc Inf Syst 20:848–856

El Sawy OA, Malhotra A, Park YK, Pavlou PA (2010) Seeking the configurations of digital ecodynamics: it takes three to tango. Inf Syst Res 21:835–848

Fiss PC (2007) A set-theoretical approach to organizational configurations. Acad Manag Rev 32:1180–1198

Fuerstenau D, Rothe H (2014) Shadow IT systems: discerning the good and the evil. In: Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel

Furneaux B, Wade M (2010) The end of the information system life: a model of IS discontinuance. Data Base 41:45–69

Furneaux B, Wade M (2011) An exploration of organizational level information systems discontinuance intentions. MIS Q 35:573–598

Furstenau D, Rothe H, Sandner M (2017) Shadow systems, risk, and shifting power relations in organizations. Commun Assoc Inf Syst 41:43–61

George JF, King JL (1991) Examining the computing and centralization debate. Commun ACM 34:62–72

Gozman D, Willcocks L (2015) Crocodiles in the regulatory swamp: navigating the dangers of outsourcing, SaaS and shadow IT. In: Proceedings of the International Conference on Information Systems (ICIS) 2015, Fort Worth, TX, USA

Greenstein SM (1997) Lock-in and the costs of switching mainframe computer vendors: what do buyers see? Ind Corp Change 6:247–274

Gregory RW, Kaganer E, Henfridsson O, Ruch TJ (2018) IT consumerization and the transformation of IT governance. MIS Q 42:1225–1253

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

Haag S, Eckhardt A (2017) Shadow IT. Bus Inf Syst Eng 59:469–473

Haag S, Eckhardt A, Schwartz A (2019) The acceptance of justifications among shadow IT users and nonusers – an empirical analysis. Inf Manag 56:731–741

Harry B, Sturges KM, Klingner JK (2005) Mapping the process: an exemplar of process and challenge in grounded theory analysis. Educ Res 34:3–13

Henfridsson O, Bygstad B (2013) The generative mechanisms of digital infrastructure evolution. MIS Q 37:907–931

Henningsson S, Kettinger WJ (2016) Understanding information systems integration deficiencies in mergers and acquisitions: a configurational perspective. J Manag Inf Syst 33:942–977

Hoffmann A, Schulz T, Zirfas J, Hoffmann H, Roßnagel A, Leimeister JM (2015) Legal compatibility as a characteristic of sociotechnical systems. Bus Inf Syst Eng 57:103–113

Huber M, Zimmermann S, Rentrop C, Felden C (2018) Conceptualizing shadow IT integration drawbacks from a systemic viewpoint. Systems 42:1–14

Köffer S, Ortbach K, Junglas I, Niehaves B, Harris J (2015) Innovation through BYOD? Bus Inf Syst Eng 57:363–375

Kopper A (2017) Perceptions of IT managers on shadow IT. In: Proceedings of the Americas Conference on Information Systems (AMCIS) 2017, Boston, MA, USA

Kopper A, Westner M (2016) Towards a taxonomy for shadow IT. In: Proceedings of the Americas Conference on Information Systems (AMCIS) 2016, San Diego, CA, USA

Kopper A, Fürstenau D, Zimmermann S et al (2018) Shadow IT and business-managed IT: conceptual framework and empirical illustration. Int J IT/Bus Alignment Gov 9:53–71

Koutsikouri D, Lindgren R, Henfridsson O, Rudmark D (2018) Extending digital infrastructures: a typology of growth tactics. J Assoc Inf Syst 19:1001–1019

Luftman J (2003) Assessing IT/business alignment. Inf Syst Manag 4:9–15

Lüker N, Winkler TJ, Kude T (2016) IT Consumerization and compliant use: do policies matter? In: Pacis 2016 proceedings

Lyytinen K, Newman M (2008) Explaining information systems change: a punctuated socio-technical change model. Eur J Inf Syst 17:589–613

Madill A, Jordan A, Shirley C (2000) Objectivity and reliability in qualitative analysis: realist, contextualist and radical constructionist epistemologies. Br J Psychol 91:1–20

Markus ML (1983) Power, politics, and MIS implementation. Commun ACM 26:430–444

Martin AW, Lopez SH, Roscigno VJ, Hodson R (2013) Against the rules: synthesizing types and processes of bureaucratic rule-breaking. Acad Manag Rev 38:550–574

Matt C (2018) Fog computing. Bus Inf Syst Eng 60:351–355
Mayer RC, Davis JH, Schoorman FD (1995) An integrative model of organizational trust. Acad Manag Rev 20:709–734
Meuser M, Nagel U (2009) The expert interview and changes in knowledge production. In: Bogner A, Littig B, Menz W (eds) Interviewing experts. Palgrave Macmillan, Basingstoke, pp 17–42
Morris MG, Venkatesh V (2010) Job characteristics and job satisfaction: understanding the role of enterprise resource planning system implementation. MIS Q 34:143–161
Nwankpa JK, Roumani Y (2014) The influence of organizational trust and organizational mindfulness on ERP systems usage. Commun Assoc Inf Syst 34:1469–1492
Panko RR (2006) Spreadsheets and Sarbanes-Oxley: regulations, risks, and control frameworks. Commun Assoc Inf Syst 17:647–676
Park Y, El Sawy OA, Fiss PC (2017) The role of business intelligence and communication technologies in organizational agility: a configurational approach. J Assoc Inf Syst 18:648–686
Pawson R, Tilly N (1997) Realistic evaluation. Sage, London
Polites GL, Karahanna E (2012) Shackled to the status quo: the inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. MIS Q 36:21–42
Raden N (2005) Shedding light on shadow IT: is Excel running your business? Hired Brains, Santa Bararba. DSSResources.com. https://cioindex.com/wpcontent/uploads/nm/articlefiles/69862-ShadowIT.pdf. Accessed 19 Jan 2020
Ragin CC (2014) The comparative method: moving beyond qualitative and quantitative strategies. University of California Press, Oakland
Recker J (2014) Towards a theory of individual-level discontinuance of information systems use. In: Proceedings of the international conference on information systems (ICIS), Auckland, New Zealand
Recker J (2016) Reasoning about discontinuance of information system use. J Inf Technol Theory Appl 17:41–66
Rezazade Mehrizi MH, Rodon Modol J, Zafar Mezhad M (2019) Intensifying to cease: unpacking the process of information systems discontinuance. MIS Q 43:141–165
Rousseau DM, Sitkin SB, Burt RS, Camerer C (1998) Not so different after all: a cross- discipline view of trust. Acad Manag Rev 23:393–404
Schlosser F, Beimborn D, Weitzel T, Wagner H-T (2015) Achieving social alignment between business and IT – an empirical evaluation of the efficacy of IT governance mechanisms. J Inf Technol 30:119–135
Silic M, Back A (2014) Shadow IT – a view from behind the curtain. Comput Secur 45:274–283
Swanson EB, Dans E (2005) System life expectancy and the maintenance effort: exploring their equilibration. MIS Q 24:277–297
Tarafdar M, Gupta A, Turel O (2015) Special issue on 'dark side of information technology use': an introduction and a framework for research. Inf Syst J 25:161–170
Urbach N, Ahlemann F, Böhmann T, Drews P, Brenner W, Schaudel F, Schütte R (2019) The impact of digitalization on the IT department. Bus Inf Syst Eng 61:123–131
Walterbusch M, Fietz A, Teutenberg F (2017) Missing cloud security awareness: investigating risk exposure in shadow IT. J Enterp Inf Manag 30:644–665
Walton RE, Dutton JM (1969) The management of interdepartmental conflict: a model and review. Admin Sci Q 14:73–84
Wilkin CL, Chenhall RH (2010) A review of IT governance: a taxonomy to inform accounting information systems. J Inf Syst 24:107–146
Winkler TJ, Benlian A (2012) The dual role of IS specifity in governing software as a service. In: ICIS 2012 Proceedings
Winkler TJ, Brown CV (2013) Horizontal allocation of decision rights for on-premise applications and software-as-a-service. J Manag Inf Syst 30:13–48
Winkler TJ, Brown CV (2014) Organizing and configuring the IT function. In: Topi H, Tucker A (eds) Computing handbook, 3rd edn. Taylor & Francis, Boca Raton, pp 57.1–57.14
Xue Y, Liang H, Boulton WR (2008) Information technology governance in information technology investment decision processes: the impact of investment characteristics, external environment, and internal context. MIS Q 32:67–96
Zainuddin E (2012) Secretly SaaS-ing: stealth adoption of software-as-a-service. In: Proceedings of the International Conference on Information Systems (ICIS) 2012, Orlando, FL, USA
Zimmermann S, Rentrop C, Felden C (2014) Managing shadow IT instances – a method to control autonomous IT solutions in the business departments. In: Proceedings of the Americas Conference on Information Systems (AMCIS) 2014, Savannah, GA, USA
Zimmermann S, Rentrop C, Felden C (2016) Governing identified shadow IT by allocating IT task responsibilities. In: Proceedings of the Americas Conference on Information Systems (AMCIS) 2016, San Diego, CA, USA
Zimmermann S, Rentrop C, Felden C (2017) A multiple case study on the nature and management of shadow information technology. J Inf Syst 31:79–101