International Journal of IT/Business Alignment and Governance
Volume 9 • Issue 2 • July-December 2018

Shadow IT and Business-Managed IT:
A Conceptual Framework and Empirical Illustration

Andreas Kopper, TU Dresden, Dresden, Germany
Daniel Fürstenau, Freie Universität Berlin, Berlin, Germany
Stephan Zimmermann, Augsburg University of Applied Sciences, Augsburg, Germany
Stefan Klotz, TU Dresden, Dresden, Germany
Christopher Rentrop, Konstanz University of Applied Sciences, Konstanz, Germany
Hannes Rothe, Freie Universität Berlin, Berlin, Germany
Susanne Strahringer, TU Dresden, Dresden, Germany
Markus Westner, OTH Regensburg, Regensburg, Germany

ABSTRACT

Research on Shadow IT is facing a conceptual dilemma in cases where previously "covert" systems developed by business entities are integrated in the organizational IT management. These systems become visible, are thus not "in the shadows" anymore, and subsequently do not fit to existing definitions of Shadow IT. Practice shows that some information systems share characteristics of Shadow IT but are created openly in alignment with the IT organization. This paper proposes the term "Business-managed IT" to describe "overt" information systems developed or managed by business entities and distinguishes it from Shadow IT by illustrating case vignettes. Accordingly, our contribution is to suggest a concept and its delineation against other concepts. In this way, IS researchers interested in IT originated from or maintained by business entities can construct theories with a wider scope of application that are at the same time more specific to practical problems. In addition, the terminology allows to value potentially innovative developments by business entities more adequately.

KEYWORDS

Alignment, Business-Managed IT, IT Governance, Shadow IT

INTRODUCTION

Shadow IT is a phenomenon that gained popularity in recent years among both academics and practitioners. It includes all software (incl. Software/Platform/Infrastructure as a Service), hardware, or IT service processes which are used or created by business units (BUs) without alignment with or awareness of the IT organization (Zimmermann, Rentrop, & Felden, 2014). The term BU in this context includes all types of business entities (individual users and business workgroups/units/departments/divisions) and is subsequently used for simplification. With the term IT organization, we refer to all

DOI: 10.4018/IJITBAG.2018070104

company-internal IT departments, subsuming different design options of the IT department(s) (Winkler & Brown, 2014). Especially trends such as cloud computing, mobile IT, and IT consumerization made it easier for BUs to procure IT by themselves without requiring deep technical expertise (Andriole, 2015; Gregory, Kaganer, Henfridsson, & Ruch, 2018). This allows BUs to become more independent from the IT organization in cases where it is perceived as too slow, too expensive, or too restrictive (Kopper, 2017). This power shift (Fürstenau, Rothe, & Sandner, 2017) undermines the control an IT organization can exert in its organization. Thus, the phenomenon can potentially lead to inefficiencies due to heterogeneous systems and uncoordinated efforts, or security-related risks with a high impact on the organization (Gozman & Willcocks, 2015).

Considering the whole body of knowledge about Shadow IT, it is mostly viewed with a negative connotation, but both researchers and practitioners are increasingly dealing with its potential benefits (Kopper, Westner, & Strahringer, 2017). It can contribute to a company's innovative potential (Silic, Silic, & Oblakovic, 2016), lead to an increased organizational agility (Tambo & Bækgaard, 2013), or simply be a way to deal with shortcomings of corporate IT systems (Alter, 2014; Behrens, 2009). These aspects stand in contrast to the negative connotation of the term Shadow IT. Also, in practice the characteristics of Shadow IT systems can change over time. As soon as the IT organization detects a hidden system it becomes visible and is not "in the shadows" anymore. The IT organization may decide to either take over control of the system completely, leave it as is, or share responsibilities with the affected BU (Zimmermann, Rentrop, & Felden, 2016). Especially a division of responsibilities as described in the latter case does not fit to the definition of Shadow IT anymore due to the involvement of the IT organization.

There is still a lack of understanding of the differences and transition between "hidden" Shadow IT systems and IT systems openly managed by BUs themselves. Behrens (2009) tries to differentiate between "good" and "bad" Shadow IT but does not systematically elaborate on their differences. Haag and Eckhardt (2017) mention "overt" Shadow IT (which is conflicting from a terminology perspective), but primarily convey a compliance perspective. There is also a phenomenon to be observed in practice that IT control is deliberately shifted to BUs. Capgemini (2016) determined that in more than 60 percent of companies, BUs were given direct control for certain IT investments (such as consulting services for pilot projects). Gartner (2017) predicts that "through 2017, 38% of technology purchases will be managed, defined, and controlled by business leaders."

The purpose of this paper is to contribute to the understanding of Shadow IT which is not "in the shadows" anymore and IT which is openly managed by BUs. For this we propose and describe the concept of "Business-managed IT" in the paper at hand to enable a more nuanced understanding of this form of IT and to relate it to organizational consequences, i.e., opportunities and risks. We also suggest consistent use of the term "Business-managed IT" for the outlined concept in the future to enable better collaboration among researchers in the field and to avoid confusion similar to all the different terms and synonyms that emerged around Shadow IT (Kopper & Westner, 2016b). This leads to our study's research question: What is the nature of Business-managed IT in organizations?

The paper is structured as follows: First, we review existing literature on Shadow IT and related topics about IT managed by BUs. Then, we define Business-managed IT and differentiate it from related concepts, followed by a detailed elaboration of our conceptual framework. After a description of the methodology, we illustrate the conceptual framework using four exemplary borderline case vignettes. Finally, we discuss the findings in relation to the conceptual framework and conclude with opportunities for future research.

BACKGROUND: FROM SHADOW IT TO BUSINESS-MANAGED IT

State-of-the-Art

To capture the state-of-the-art of academic research around the proposed concept of Business-managed IT, we conducted a literature review (Levy & Ellis, 2006). As search keywords we used a combination

of shadow, feral, workaround, un-enacted, unsanctioned, rogue, and grey with IT, systems, and projects. Moreover, the terms bottom-up IT, Business-managed IT, end-user development, and user-driven innovation were included in the search. The search keywords were applied to title, abstract, and keywords querying AIS Electronic Library, Business Source Complete (EBSCO), Emerald Insight, IEEE Xplore, ScienceDirect (Elsevier), and SpringerLink. In addition, backward/forward reference and backward/forward author search was conducted. The literature search identified 107 relevant publications after deduplication and removal of irrelevant papers.

Three related themes exist in the identified publications: Causing factors, outcomes (i.e., benefits and risk/shortcomings), and governance of Shadow IT and Business-managed IT (Klotz, Kopper, Westner et al., 2018). Governance measures depend on whether IT instances (i.e., software, hardware, or services) are known or hidden. In addition to general governance measures, more specific governance measures exist if instances are not hidden ('overt').

Earlier literature on Shadow IT and related concepts focused on causing factors (Klotz, Kopper, Westner et al., 2018). Causing factors include enablers, motivators, and missing barriers. Shadow IT and Business-managed IT is enabled by improved accessibility, i.e., it becomes easier for BUs to deploy/procure IT solutions (Spierings, Kerr, & Houghton, 2017), e.g., due to cloud offerings (Haag & Eckhardt, 2017), or smartphones (Davison, Ou, & Chang, 2018). In addition, IT user competence increases in BUs. For example, digital natives, who grew up using IT products extensively (Rentrop & Zimmermann, 2012b), are employees with increased IT skills today. Missing business-IT-alignment as well as shortcomings of the existing IT instances are major motivational factors for Shadow IT and related concepts (Klotz, Kopper, Westner et al., 2018). Business-IT non-alignment takes the form of lacking business knowledge in the IT organization (Fürstenau et al., 2017), which can lead to unmet user needs (Khalil, Winkler, & Xiao, 2017), detrimental experiences of the BUs with the IT organization over time (Zimmermann & Rentrop, 2014), and subsequently a low level of trust between BUs and the IT organization (Zainuddin, 2012). Existing IT shortcomings include their inflexibility and complexity (Ortbach, 2015), insufficiency (Huuskonen & Vakkari, 2013), or even malfunctions and errors (Kent, Houghton, & Kerr, 2013). Shadow IT and Business-managed IT can also be driven by employee motivation/goal orientation (Haag & Eckhardt, 2015), a lack of agility of the IT organization (Khalil et al., 2017), anticipation of a beneficial cost structure (Fürstenau, Sandner, & Anapliotis, 2016), and business environment uncertainty (Zimmermann, Rentrop, & Felden, 2017). Lacking restrictions, such as non-existing or insufficient policies (Silic & Back, 2014), as well as lacking awareness (Dittes, Urbach, Ahlemann, Smolnik, & Müller, 2015) are missing barriers which could otherwise prevent deployment of IT instances autonomously in BUs.

Outcomes of Shadow IT and Business-managed IT can be benefits (i.e., positive outcomes), as IT activities managed by BUs are generally intended to benefit the organization (Buchwald, Urbach, & Ahlemann, 2014b), as well as risks/shortcomings (i.e., negative outcomes). Academic research describes productivity gains as a potential benefit, e.g., due to improved efficiency (Röder, Wiesche, & Schermann, 2014) and effectiveness (Walterbusch, Fietz, & Teuteberg, 2017) which is mainly driven by productivity gains of individual employees (Haag, Eckhardt, & Bozoyan, 2015). Moreover, Behrens (2009) highlights that Shadow IT can be a powerful source of creativity and innovation as it leverages users' innovation potential (Silic et al., 2016). Further potential benefits mentioned in literature are enhanced agility (Khalil et al., 2017), increased flexibility (Zimmermann et al., 2017), improved user and customer satisfaction (Ferneley, 2007; Singh, 2015), and intensified collaboration (Behrens, 2009). If IT activities in BUs happen overtly, risks/shortcomings are more transparent and, in contrast to hidden Shadow IT, might subsequently be better mitigated (Klotz, Kopper, Westner et al., 2018). Hence, risks/shortcomings of Shadow IT are well covered in academic research (Kopper & Westner, 2016a). Shadow IT poses risks for security (Khalil et al., 2017) and data privacy (Röder et al., 2014). A lack of integration (Hetzenecker, Sprenger, Kammerer, & Amberg, 2012) might lead to data inconsistencies (Györy, Cleven, Uebernickel, & Brenner, 2012; Kretzer & Maedche, 2014), which can result in a loss of credibility (Myers, Starliper, Summers, & Wood, 2017). Furthermore,

Shadow IT can contribute to inefficiencies due to loss of synergies or scale effects (György et al., 2012), e.g., due to redundancies (Chua, Storey, & Chen, 2014). Eventually, Shadow IT might contribute to a loss of control, undermining IT governance (Khalil et al., 2017), management intentions (Röder et al., 2014), and strategic goals (Chua & Storey, 2016), as well as to a lack of continuity, e.g., due to a lack of documentation (Fürstenau et al., 2017) and dependence on few employees (Behrens, 2009).

There is also a theme that focuses on aspects of governance of IT autonomously employed in BUs, which has been the focus of recent research (Klotz, Kopper, Westner et al., 2018). General governance measures include the setup of policies (including bring your own device (BYOD) policies), awareness training, monitoring and identification, as well as IT gap resolution. A prohibition of Shadow IT and Business-managed IT might not be reasonable because valid causing factors for the business-deployed IT might exist (Chua & Storey, 2016) and because it would prevent benefits of the phenomenon (Köffer, Ortbach, Junglas, Niehaves, & Harris, 2015). Hence, some IT managers actively enable Business-managed IT under certain conditions (Kopper, 2017). Nevertheless, awareness creation of existing policies seems beneficial, e.g., aiming for a minimization of potential risks of unapproved IT (Haag, 2015; Walterbusch et al., 2017). Moreover, technical monitoring can enforce policy adherence (Silic & Back, 2014) and can be one possibility to identify Shadow IT (Zimmermann et al., 2014). A reduction of IT systems shortcomings might fulfil unmet user needs and reduce the demand of BUs to deploy IT autonomously (Walterbusch et al., 2017; Zimmermann & Rentrop, 2012). If an IT instance created by a BU is known to the IT organization more specific governance measures exist: The instance can be categorized, its continuation or decommission can be determined, and subsequently the governance of the instance can be allocated between the IT organization and the BU (Klotz, Kopper, Westner et al., 2018). Multiple instance categorization approaches exist, e.g., by criticality and quality, by functional scope and scope of use (Rentrop & Zimmermann, 2012a). The categorization of an existing Business-managed IT instance is beneficial for the allocation of its governance (Klotz, Kopper, Westner et al., 2018). If instances are continued their governance can be allocated to the IT organization (Zimmermann et al., 2017), the business unit (Andriole, 2015), or in a split responsibility model (i.e., instance co-governance) (Gregory et al., 2018). The governance allocation is similar to the principle of horizontal allocation of decision rights (Winkler & Brown, 2013). Zimmermann et al. (2016) study the allocation of IT task responsibilities between the IT organization and the BU of Business-managed IT and are, thus, describing case studies of Business-managed IT co-governance. However, a co-governance model can also be chosen to generally govern the creation and management of IT activities in BUs. In a co-governance setup, collaboration and knowledge exchange (Peppard, 2016) as well as systems and platforms embrace end-user IT or development (Gregory et al., 2018). Bygstad (2017) describes generative innovation with lightweight IT in form of small innovative apps which are created by users on platform systems, for example BI platforms (Kretzer & Maedche, 2014). Sedera, Lokuge, Grover, Sarker, and Sarker (2016) also find that enterprise system platforms have a significant impact on innovation in organizations.

While the three identified themes describe aspects of both ("hidden") Shadow IT and IT activities managed by BUs ("outside the shadow"), they do not sufficiently describe the differences and transition between them. The following sections therefore define the term Business-managed IT and aim to address this gap by outlining and demonstrating a conceptual framework.

Phenomenon and Terminology

During our previous research in the field of Shadow IT, we saw instances of hidden Shadow IT which were made visible in an organizational IT management context and became subsequently legitimized (Zimmermann et al., 2017). In these cases, the term Shadow IT would not apply even if the instance is still managed by the respective BU as before. We also saw information systems (IS) which shared all characteristics of Shadow IT, but which were openly managed by a BU in agreement with the organizational IT management (Kopper, 2017). We refer to Shadow IT systems, and more generally

IS, as socio-technical systems, recognizing the interaction between social and technological systems (Winter, Berente, Howison, & Butler, 2014).

To gain a better understanding and to appropriately define this type of Business-managed IT, we analyzed several concepts that have been discussed in the past in a related context: "End-user Computing" (Panko & Port, 2012) historically describes independent usage of IT systems by end users, not including the creation of new sophisticated IT artifacts, but possibly of small and simple solutions developed with end user tools such as spreadsheet applications. Furthermore, its focus is on individual users rather than whole BUs. "Workarounds" (Alter, 2014) primarily describe goal-driven adaptations or modification of existing socio-technical systems without changing their overarching architecture (Lund-Jensen, Azaria, Permien, Sawari, & Bækgaard, 2016). "Decentralized IT" (Winkler & Brown, 2014) represents multiple divisional IT units separate from BUs. "Bring Your Own Device" (Köffer et al., 2015) is related to Business-managed IT in the way that usage of individually owned devices is aligned with the IT organization, but it does not include all kinds of IS.

Some other alternative terms used in practice which are related to the concept of Business-managed IT were considered. "Citizen IT/development" (TechTarget, 2016) is used to describe users of low-code platforms and is limited to this area. "Embedded IT" (TechTarget, 2014) deals with the attachment of IT staff members to BUs and does not include non-IT staff. Gartner's (2016) "Business Unit IT" has some resemblance to Business-managed IT but is used inconsistently. Other possible terms were also discussed, such as "Business-driven IT/innovation" (György et al., 2012) which might be confusing as all IT should inherently drive business value. This similarly applies to "User-driven IT/innovation" (Fürstenau & Rothe, 2014) but with a focus on users rather than BUs. In the following conceptual framework, we therefore finally settle on the term Business-managed IT to highlight the task responsibility aspect from a governance and managerial perspective.

Conceptual Framework

Concluding the definition section, the involvement in organizational IT management provides one parameter to distinguish Business-managed IT and Shadow IT. Regarding this, we differentiate overt and covert IS (Ferneley, 2007; Haag & Eckhardt, 2017). Both terms are etymologically related to the French "ouvert" (open) and "couvert" (covered). We define an IS as overt, if the related activities regarding its development and operation are practiced openly. This means that relevant stakeholders (e.g., business management, senior management, and/or official IT organization) are aware of the system, monitor these activities and enforce existing controls. Conversely, we define an IS as covert, if related activities are practiced in a hidden form (Spierings, Kerr, & Houghton, 2012). Relevant stakeholders do not know that it exists, and it is not controlled and monitored. Thus, covert IS, which represent the implicit focus in research on Shadow IT, are not involved in given IT management controls of a company. Depending on a company's IT management maturity they are neither registered nor strategically planned within organizational IT management processes (Boynton, Zmud, & Jacobs, 1994) such as IT service management (Zimmermann & Rentrop, 2014) or enterprise architecture management (Fürstenau & Rothe, 2014; Huber, Zimmermann, Rentrop, & Felden, 2017; Tambo & Bækgaard, 2013).

While covert and overt IS suggest a clear distinction, we assume that several "shades" exist, i.e., there is a continuum of occurrences. These shades describe different levels: At first, the management level of a company may have no awareness about a system's existence at all. One step further, board members or IT managers may have some minor information that a business workgroup or end user operates an own system. Finally, a covert system may be taken for granted without its registration and consideration in an operational or strategic IS management context (Zimmermann et al., 2017). Thus, there seem to exist borderline cases that can be partly overt as well as covert, which suggests a continuum between a covert and an overt IS.

Another parameter to differentiate IS in this context relates to IT task responsibilities and considers the concept of application governance which consists of two dimensions of IT decision rights - decision

authority and task responsibility (Winkler & Brown, 2013). While the former addresses the allocation of application decision rights mainly from a superior IT function perspective (such as investment or architecture planning), the latter allocates the actual execution of operations on the single application or IT service level (e.g., the development and maintenance of infrastructure, databases and application programs as well as IT service processes) (Winkler & Brown, 2013; Zimmermann et al., 2016). Historically, IT governance focused largely on the allocation of decision authority for IT (Weill & Ross, 2004). Recently, the question of allocating task responsibilities arose (Winkler & Brown, 2013). Thereby the question is not only interesting in the context of outsourcing and participatory governance between internal and external stakeholders (Andriole, 2015). It extends to internal relationships between BUs and IT organizations (Chua & Storey, 2016). In this paper, IT task responsibility is characterized by the allocation of application governance between the BU and the IT organization and is therefore distinct from the organizational setup of the IT organization. The organizational setup of the IT organization in corporations can range from centralized to decentralized, including intermediate setups such as hybrid variants (Brown & Magill, 1994; Winkler & Brown, 2014). In our definition, IT task responsibility in the BU describes human resources that do not belong to the IT organization but perform IT-related tasks. In contrast to that, decentralized organizational IT setups describe human resources that belong to the IT organization (for example a local IT organization in a global enterprise).

Studies describe organizational behavior to deal with Shadow IT by retaining related tasks in the BU or by transferring responsibilities for the system to the IT organization (Beimborn & Palitza, 2013; Chua et al., 2014; Zimmermann et al., 2017). Product-related IT, shop-floor IT, or small, non-critical solutions illustrate typical examples with responsibilities given to the BU (Fürstenau & Rothe, 2014; Kopper, 2017). As organizations in these cases often strive for some central control (Chua & Storey, 2016; Kopper, 2017), different shades exist for the parameter of responsibility allocation (Winkler & Brown, 2013). Organizations divide IS into subtasks and components and allocate task responsibilities between BUs and IT organizations (Zimmermann et al., 2016). Thereby, they share responsibilities for a system – for example by transferring hardware or database components of a former Shadow IT instance to the IT organization (Chua et al., 2014; Kopper, 2017; Zimmermann et al., 2016). Thus, also for this parameter a continuum exists for allocating tasks between BUs and IT organizations with regard to shared responsibilities.

Combining the two governance parameters involvement in organizational IT management (overt/covert) and task responsibility between BUs and IT leads to a matrix as shown in Figure 1. Thereby, we can differentiate three types of IS:

- **Business-Managed IT:** Describes overt IS from an organizational IT management perspective with a high degree of responsibility for IT components and tasks in the BUs. In detail, we therefore define Business-managed IT as all software (incl. Software/Platform/Infrastructure as a Service), hardware, or IT service processes which are overtly created/procured or managed by business entities (individual users, business workgroups, or business units) either in alignment with the IT department or in a split responsibility model;
- **Shadow IT:** Describes covert IS. It typically exists in BUs with the respective functional responsibility. However, Shadow IT in the IT department is also possible, e.g., when IT employees develop own covert IT or when they support Shadow IT in BUs, e.g., by providing interfaces or services not involved in organizational IT management;
- **IT-managed systems:** Describe the traditional IT landscape of enterprise systems: Overt systems, controlled within the organizational IT management, with a high degree of responsibility for IT components and IT tasks such as planning, engineering or sourcing, testing, documenting, operation, etc. in the IT department.

While prior research concentrates on the term Shadow IT and IS managed by the IT department, a detailed study of Business-managed IT is missing. However, it seems necessary to structure discussions in research and practice regarding the described governance parameters. A detailed description of the term Business-managed IT could help in this debate. Thereby, the borderline cases regarding partly overt/covert systems and shared responsibilities between business and IT are of special interest.

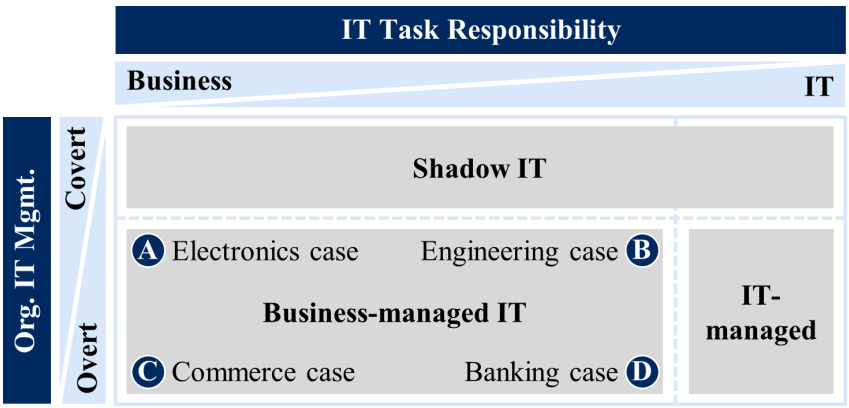
METHODOLOGY

To illustrate and refine our concept empirically, we present four cases on Business-managed IT as indicated in Figure 1. The examples were extracted from three broader studies conducted by different researchers (the authors). Zimmermann, Rentrop and Felden (2017) (describing cases A and B) focused on four case studies with 40 interviewees from BUs and IT organizations to analyze the nature and management of Shadow IT in companies. Fürstenau and Rothe (describing case C) have conducted an exploratory study in the retail industry to investigate the nature of business-driven systems. Data on the development of an e-commerce system was collected over a period of six years, including seven interviews, several days of on-site observations, and an analysis of 86 company documents. Finally, Kopper (2017) (describing case D) has conducted a study based on 16 interviews with executive or senior IT managers to get an up to date IT management's perspective on Shadow IT. From these studies, we selected four examples which match our focus on borderline cases in the sense of extreme cases (Seawright & Gerring, 2008; Yin, 2013, p. 178). All companies described in the cases are located in Europe.

For each individual example (case), one or more IT solutions were chosen as the unit of analysis and existing qualitative data from the respective research study was revisited. Depending on the individual case, data included interviews, observations (from which field notes were taken), and archival materials. For some cases, additional data was collected for the paper at hand to close obvious gaps in the data. A case database was created in a spreadsheet program to document the cases.

To analyze and present our results, we utilized the technique of case vignettes (Yin, 2013, p. 178). Case vignettes can be defined as a variant of the case method where a particular case of interest is prepared and presented in a brief, illustrative manner. A case vignette outlines the salient features of the case, the observed line of management and rationales for why certain decisions were made by the actors involved. The method's value lies in a structured representation of the case that can foster discussion among researchers and practitioners. Within several iteration rounds, the cases were discussed and mutually evaluated within the team of authors.

Figure 1. Conceptual framework and case vignettes describing borderline occurrences of business-managed IT



In connecting our discussions to prior research and using multiple sources of evidences we ensured high construct validity regarding the studied concept of Business-managed IT. Pattern matching within and across the case vignettes guaranteed internal validity; the mutual confirmation of single case results by the different researchers involved in this paper as well as the replication and comparison of results across different industries raised external validity. The usage of interview protocols and a case vignette database ensured a high reliability (Yin, 2013).

EMPIRICAL ILLUSTRATION OF BUSINESS-MANAGED IT THROUGH CASE VIGNETTES

In this section we describe four case vignettes of Business-managed IT in different industries (Table 1). For each case we provide a brief description of the context, its history/lifecycle, and a diagnosis of the dimensions "Organizational IT management" and "IT task responsibility". We also describe rationales for the chosen line of management, which includes potential opportunities and risks.

(A) Electronics Case (Partially Overt and Business Responsibility)

The first case vignette is situated in a marketing workgroup of an electronics company, which experienced an intense growth in the recent years before the point of analysis.

In this company, marketing employees had to manage internal and external participants during a fair or exhibition. This included scheduling meetings between sales representatives and customers, tracking these meetings, and recording conversation results. Marketing staff was overwhelmed by the increasing work. As there was no suitable IS and marketing had previously experienced resource bottlenecks in the IT organization, they began to search for a solution by themselves. As a result, they sourced a software as a service for event management. The system provided a booking portal that could be adapted to the needs of the marketing group. To transfer the lead and client data captured during the event into the company's customer relationship management system, they used spreadsheets.

Table 1. Case vignettes describing borderline occurrences of business-managed IT

		Case Name (Pseudonym)			
		(A) Electronics	**(B) Engineering**	**(C) Commerce**	**(D) Banking**
Company	Industry	Electronics industry	Engineering industry	Retail industry	Financial services
	Location	Germany	Germany	Germany	Germany
	Staff	>5.000	>10.000	>10.000	>10.000
	Sources of evidence	Interviews with business & IT managers and document analysis	Interviews with business & IT managers (incl. CIO); document analysis & observations	Interviews with project leads, analytics managers, and contextual observations	Interview with CIO and contextual background information
Case	System(s)	Event management system	Order management system	Web shop system	Self-service integration platform, development platform, CRM
	Org. IT mgmt.	Partially overt	Partially overt	Overt	Overt
	IT task responsibility	Business responsibility	Shared responsibility	Business responsibility	Shared responsibility

At the point of analysis, the system was still in a prototype stage with about ten users and unclear future usage scenarios. While the IT organization started processing several other IT projects in the marketing department, IT managers became aware of the system's existence.

This case describes an IS that is partially integrated into the organizational IT management and thus contains covert and overt elements. While several stakeholders (such as some IT, marketing, and sales managers) knew and recognized the system, others were not aware of it, e.g., marketing management itself or the compliance department. Furthermore, it was neither actively monitored nor any controls existed or were enforced regarding quality and criticality issues. An IT project manager responsible to support marketing systems stated "I know that my business colleagues procured an online tool to organize their events. But I do not have detailed insights or started to monitor it. However, due to a few risks I see, we need to find a way how to deal with this solution." Regarding IT task responsibility, the marketing workgroup executed all tasks related to the system, such as sourcing, adapting the system, and maintaining it.

The chosen rationale of management in form of Business-managed IT resulted from missing systems and resources provided by the IT organization and a high uncertainty regarding future usage. Furthermore, the event management system had a mixed task specificity "incorporating standardized and customized elements" (McIvor, 2009), which emphasized a strong relation of partial tasks better retained on the BU side. This and uncertainty aspects supported a form of governance with retaining task responsibilities on the BU side. A member of the IT organization stated, "There is no necessity to spend resources from the IT organization's side until the business side is certain about future usage. If it is more certain it may become the task of the IT unit to provide an appropriate interface to core systems." This also shows that a necessity for greater overtness arose. Management demanded consideration of compliance aspects such as the protection of client and employee data in the system. Therefore, the company strived to embed the solution in the organizational IT management and provide controls, but without restricting business creativity and responsibility.

(B) Engineering Case (Partially Overt and Shared Responsibility)

The second case vignette originates is situated in the context of a manufacturing plant belonging to a large engineering company. In this company, a central IT organization is accountable to provide IT services to several manufacturing plants and sales offices in Europe.

A workgroup of employees from the engineering and construction department started to self-develop an order management system in the early 2000s. In the following years, the initially small system grew to a large web-based system with several hundred users. With highly specific construction drawing, order scheduling, and calculation functionalities the system to date still supports the order management process of sales representatives and engineers. After initially running the system on a physical server on their own premises, the workgroup started to host the system on servers from external providers. At the beginning, data was uploaded manually into the enterprise system provided by the IT organization. When more relevant stakeholders became aware of the system, criticality demanded a transfer of the main server infrastructure to the IT organization. Furthermore, the IT organization provided connectors for interfaces to the enterprise system to enable automation.

At the point of analysis, the order management system and its components were only partially involved in organizational IT management. The case describes overt and covert IT activities in the BU with shared task responsibilities due to some tasks transferred to the IT organization. It describes a typical example of a historically grown Business-managed IT system. Starting in the (covert) shadows due to non-existing IT solutions and due to innovative ideas in the BU, the functional scope and the number of users gradually increased. As a result, the system was taken for granted by managers in the manufacturing plant and in the sales offices. While the system thereby became institutionalized and the infrastructure workgroup of the central IT organization started to provide servers and interfaces, IT management as a whole only had minor information about the system itself, and the associated

activities. An IT manager stated "we do not really know for which processes and to what extent the self-implemented system is used. It is definitely not properly included in organizational IT management."

Providing a system in the BU for order management increased productivity and IT managers acknowledged the innovative nature. One IT manager stated, "This system includes innovative technologies and procedures for the manufacturing plant. Without it, the sales and engineering process would be much more complicated." The fact that highly business-specific skills are necessary for parts of the system regarding the programming of drawings, calculations, etc., supported the chosen rationale of management to retain most task responsibilities on the business in the BU for efficiency and agility reasons. An IT manager stated, "I do not see a chance to establish this unique, business-specific knowledge in our department. Therefore, these specific tasks related to this IT system are better kept on the business side." However, the system includes high security risks and IT standardization intentions are hindered, leading to inefficiencies. Thus, the company strived for more control - by involving more components and activities in organizational IT management - and a restructuring of task responsibilities. Business and IT managers decided to transfer, e.g., database- and server-related tasks and access control procedures to the IT organization. Thus, the IT-managed part increased. Furthermore, to gain quality the company strengthened collaboration between BUs and the IT organization. By increasing overtness and shaping an interdisciplinary governance of shared responsibilities, managers aimed for a Business-managed IT model with a better balance of innovation potentials and related risks and inefficiencies.

(C) Commerce Case (Overt and Business Responsibility)

The third case vignette is situated in the context of a large commerce company, which has transformed from a catalog shipper with complementary digital services to an e-commerce-first company in recent years.

In 2011, the e-commerce department began to independently develop a web shop system. The department was commissioned by the board to prepare the system. It finally went live in 2013 and today processes more than 90% of the company's order volume (2.7 billion Euros, up to ten orders per second). The system's development was based on agile principles (such as scrum, interdisciplinary teams, self-organization, open source development, etc.) and followed design rules of a modular architecture (i.e., microservices have been used since 2015).

In this case, Business-managed IT was overt. The system is largely known to both the company's board of directors, other BUs in the same subsidiary and to the IT organization. The board provided a double-digit million Euro budget to build the system, and at a later stage, resources for further development. The e-commerce department is completely responsible for the development and management of the system. The project started with a team of 100 staff members (programmers, test managers, UX and design specialists, project and product managers, etc.). Since then, it has grown to its current size of 250 employees. The department is organized in interdisciplinary development teams across functional areas (search, navigation, product presentation, etc.). The teams are organized as "standing teams" and are integrated into line management of its related BU via product managers. The department has adopted its own architectural and organizational principles. It is completely detached from the central IT organization which - as a service center - provides standardized services to all companies of the group. By defining architectural principles within the BU at the macro level (e.g., "RESTful architecture", or "central responsibility for data and data supply processes") and at the micro level (e.g., "buy when not core", or "common basic technologies") it is attempted to ensure that redundancies remain controllable and the architecture does not erode.

The main reason for the selected strategy was that it enabled the BU to progress with increased agility. The company operates in a turbulent environment and the future market development was and remains difficult to predict. In the words of the initiative leader: "You don't even know what you want to do with [system name], you don't even know what e-commerce will be like in five years, so let's build an organization and process landscape that enables [company name] to react to change." In addition,

timing was favorable. After an attempt to consolidate the IT landscape across all group companies had failed, the board was open to give IT decentralization a try. At the same time, the position of the IT organization was weakened. The BU could take advantage of the opportunity to build a successful system. Nevertheless, it demanded constant institutional work (by relentless individuals) to justify the detached position within the company. On the one hand, the board had to be repeatedly convinced that pursuing the project was worthwhile. On the other hand, the position and the benefits within the group had to be justified to defy the arguments for centralization by the other BUs and the central IT organization. With increasing momentum, the sentiment began to turn slowly, and other departments within the company began to orient themselves to the agile principles of the department.

(D) Banking Case (Overt and Shared Responsibility)

Banking Case vignette is situated in a commercial banking company and based on an interview with the CIO. In this case, the IT organization introduced a self-service integration platform which allows BUs and users to integrate their own applications and to have controlled access to data of other systems. In this shared responsibility model, the IT organization takes care of the technical data integration layer with the core systems and manages the security aspect of the platform. BUs can make use of the graphical interface of the platform which does not require deep technical expertise and use it, for example, to extract data for further usage in other reporting applications. There is also a ruleset which defines which data is read only and which data can be fed back into core systems. A predefined entity in one of the BUs is responsible for data quality and data governance. BU activities are principally overt as the platform automatically provides documentation and logs, i.e., visibility, of the integration.

At the time of the interview, the IT organization was also building a central .NET development environment as a platform for Business-managed IT. The environment will be secured centrally and will also, for example, provide built-in backup functionalities. BUs will have to use this platform for their developments and must agree to adhere to a defined set of programming, architecture, test, documentation, and authorization concept guidelines to fulfil regulatory requirements. One example for such a case (from which the platform originally emerged) is a small pricing system which was developed and is maintained by some traders in the capital BU (together with an external vendor) in close alignment with the IT organization. They adhere to predefined, agreed upon processes, use tools provided by IT, and work with IT for testing and go-live on the infrastructure run by IT.

The organization was also in the process of consolidating multiple systems (from different branches) into a single cloud-based CRM and establishing a shared responsibility model to maintain it. Some resources in the largest BU with the most complex requirements (corporate banking) would take care of maintenance, parametrization and further development of the system (including requirements management and implementation). The same BU would also coordinate requirements with other BUs and enable synergies. For topics such as integration with other systems (for example, email system) the BUs would still need to adhere to official processes and work together with IT. The IT organization also stays in control of contract management, security, and budget.

All these setups were chosen to allow for a more agile development of systems and a better coverage of users' needs. BUs can develop their own systems based on their deep understanding of their own processes and they do not have to go through complex project requests with the IT organization. Still, the interviewee expects increased costs due to potential inefficiencies as a downside and notes that this model requires that responsibilities are clear and adhered to. It also assumes that all BUs deal with IT systems only on a level which requires less technical expertise. This is accomplished by providing platforms that are controlled by the IT organization or largely managed by a professional provider as in the case of the cloud-based CRM, which also reduces operational continuity risks. For the interviewee, this split model is rather feasible in the "new world", i.e., with the availability of SaaS, and not in the "old world" where expert level IT skills are required to operate systems. While SaaS also makes it easier for BUs to procure systems on their own, they increasingly understand that the IT organization needs to be involved in the process.

DISCUSSION

The next section discusses our findings in relation to our research question and the conceptual framework. We focus on the nature of Business-managed IT in organizations, discuss the dimensions of overtness and responsibility, and take a position on the discussion about beneficial and disadvantageous characteristics of Business-managed IT from various perspectives.

In this paper, we have proposed to define Business-managed IT as overt IS - involved in organizational IT management - for which task responsibility lies with business entities (individual users, business workgroups, or business units). In contrast to Shadow IT, Business-managed IT is overt, meaning it is known to and monitored by important stakeholders. In contrast to IT-managed systems, responsibility for tasks lies (at least in part) with the business entities. Four examples illustrated different types of Business-managed IT and acted as cases for the discussion of borderline areas.

Discussion of "Involvement in Organizational IT Management"

Our cases range from complete overtness in the sense of known and officially monitored solutions (C, D) to cases which include covert elements (A, B). It therefore becomes clear from our case vignettes, that overtness (Ferneley, 2007; Haag & Eckhardt, 2017) is a multifaceted construct. First, overtness can be understood in terms of who is aware of and knows something about an IT solution. Secondly, however, it also plays a role which IT management processes are established in the organization and whether the IT solution is registered in and monitored by them. Examples for such processes are strategic and tactical planning (including architecture, security, and audit) (Boynton et al., 1994), or project portfolio management (Daniel, Ward, & Franken, 2014). In this context, awareness of Business-managed IT and the utilization of these processes influence each other. This relation builds the basis to be able to exert control.

Some systems, such as the web shop system in the commerce case (C) or the systems in the banking case (D), were fully known to relevant stakeholders. This includes top management, which assures the approval of resources and support, and the IT organization, which was aware of the IT system. Other examples from our cases were partially covert. We discussed the event management system in the electronics case (A): While some stakeholders (e.g., relevant IT and sales managers) knew and valued the system, others were not aware of it. The order management system in the engineering case (B) illustrates how IT management started with passing knowledge of the system, until it became eventually known and monitored. Altogether, in this context, overtness can thus be understood as the degree to which key stakeholders know about (are aware of) an IT system. Business-managed IT differs from Shadow IT in that, among other things, shadow spaces are opened up and a system is made known and managed.

Registration in and monitoring by certain IT management processes is often a prerequisite for awareness. Following work by Power (2007), organizations are in a process of making uncertainties known and thus making them manageable by transforming "uncertainties" into manageable "risks." According to this view that evolved in the context of enterprise risk management, companies regain a certain degree of control over things that would otherwise not be controllable by assigning and monitoring performance indicators. To do so, they have devised "instruments of seeing" (e.g., enterprise risk management), which allow to perform these monitoring tasks on an enterprise scale (Buchwald, Urbach, & Ahlemann, 2014a). Similarly, enterprise architecture management, IT compliance management, IT portfolio management, IT security management, and IT service management can be understood as "instruments of seeing" in the context of Shadow IT and Business-managed IT. They allow to focus on or see things that would otherwise be amorphous. In this sense, overtness can be understood as the degree to which a system is monitored by processes on an enterprise scale. Whereas Shadow IT tends to be unmonitored and unregistered, Business-managed IT tends to be registered and monitored.

Discussion of "IT Task Responsibility"

The diverse occurrences of IT task responsibilities in our case vignettes provide two other insights into the nature of Business-managed IT. First, our findings support that Business-managed IT implies responsibilities in BUs for operating IT tasks of IS. Second, the case vignettes show different options how organizations shape the governance of IT task responsibilities in BUs with regard to control and responsibility by the IT organization (Brown & Magill, 1994).

In a setup with traditional roles, BUs raise IT requirements that the IT organization is supposed to meet (Winkler & Brown, 2014). However, this is not the case in all our examples and potentially subject to a change. Driven by new ideas and technological possibilities, BUs and users themselves design and implement IS. Shadow IT and other examples from literature such as product-related IT or shop-floor IT (Kopper, 2017) support this argument.

The responsibility for Business-managed IT tasks goes along with the question of how far the responsibility reaches and refers to the research discussion on application and IT service governance. This affects the allocation of responsibilities between BUs and IT organizations on a single IS level (Chua et al., 2014; Winkler & Brown, 2013; Zimmermann et al., 2017). While in the commerce case (C) and in the electronics case (A) BUs are entirely responsible to operate IT tasks, the engineering (B) and the banking (D) case examples describe a differentiated way of task allocation. In the latter cases, the analyzed companies shared the responsibilities for sub-tasks and components between BUs and IT organizations. The engineering case (B) underlines management approaches for dealing with Shadow IT (Chua et al., 2014; Kopper, 2017; Zimmermann et al., 2016) as the company transferred non-specific, critical tasks (for infrastructure, database, and other security-relevant activities) to the IT organization. The banking case (D) demonstrates this in a similar way with the difference that already from the beginning overt IS were operated with shared tasks between BUs and IT organizations.

Agile practices (e.g., Scrum, feature-driven development, extreme programming) currently change the ways, by which IT is developed and operated in companies, aiming to improve their software development (Chow & Cao, 2008). Hence, this paper understands agile practices as methodological practices for IS deployment opposing traditional development methodologies, such as waterfall. As a result, Business-managed IT, Shadow IT, and IT-managed instances could be developed in an agile or in a traditional way. However, the usage of agile practices in IT deployment increases the business-IT alignment, e.g., due to collaboration between business people in agile projects (Beck et al., 2001), and agility, e.g., due to frequent software delivery (Beck et al., 2001), which addresses root causes for Business-managed IT and Shadow IT (Klotz, Kopper, Westner et al., 2018).

Discerning the Good and the Bad of Business-Managed IT

Similar to Behrens' (2009) differentiation between "the good, the bad, and the ugly" of Shadow IT, we also discern beneficial and disadvantageous characteristics of Business-managed IT. As we discussed in the previous section, overtness (visibility or awareness in its most basic form) is a necessary characteristic to be able to evaluate and manage the risks of IT systems. This contributes to a "positive" notion of Business-managed IT in contrast to Shadow IT, which may impose unmanageable risks due to its covert nature. However, not all overt developments in BUs are necessarily positive, as they may also be harmful if they arise in deliberate opposition and as a demonstration of power by the BUs (against a powerless IT organization) (Spierings et al., 2012). Nevertheless, as discussed in the previous section, tasks for uncovered Shadow IT can be transferred to the IT organization based on a criticality and efficiency assessment (case B) (Zimmermann et al., 2016). The decision factors for dealing with and allocating tasks for uncovered Shadow IT (i.e., opportunities and risks) can also be adapted to the concept of Business-managed IT. While our cases show that such a setup is motivated by opportunities for increased agility, it also aims to mitigate associated risks by providing a controlled environment for critical components/tasks such as infrastructure and security (case D). This kind of responsibility split is similar to the hybrid model described by Brown and Magill (1994) where "management of technology" is centralized and "management of use of technology" is decentralized.

Especially for cases where task responsibility lies predominantly with BUs (C), external control (through the IT organization) is replaced by other forms of control. On the one hand, self-control (through the BU) has a stronger importance and the BU is empowered. On the other hand, improved monitoring and control solutions (e.g., cloud access security broker, activity monitoring, or application delivery controller) are used to retain transparency (Fernandez, Yoshioka, & Washizaki, 2015). In some constellations, coordination mechanisms are also required. In the case of pure Business-managed IT, empowerment is total, and the BU is almost completely decoupled from the IT organization (C). The IT organization needs to take on a different role in such a constellation and act as a trusted advisor and partner to the business (Kopper, 2017). The definition of rules is (almost) completely left to the department which coordinates and synchronizes within the organization (for example, with other departments). An advantage of this setting is an increased level of speed and agility, fostered by a minimum degree of restrictions and processual overhead or transaction costs (Zimmermann et al., 2014). A disadvantage is the potential duplication of services and the resulting increased costs due to inefficiencies (Blichfeldt & Eskerod, 2008). However, to a certain degree this is an accepted trade off as shown in our case vignettes.

CONCLUSION

To conclude, our aim was to introduce the concept of Business-managed IT to the debate around Shadow IT and more generally IT solutions procured, developed, or maintained in BUs. Business-managed IT - defined as overt IT solutions within the area of BU responsibility - makes it possible to realize advantages which have been primarily associated with Shadow IT (e.g., agility, lower load on official IT, autonomy in departments), while it promises to avoid some of the disadvantages (e.g., missing transparency, data protection risks, IT security and regulatory compliance risks, loss of control and cost explosion). The case examples presented in our paper demonstrate the potential of Business-managed IT in aiming to balance the tension between speed/autonomy and cost-effectiveness/safety/risk. Business-managed IT with a shared responsibility model also reflects a new interdisciplinary way of collaboration between business and IT organizations (Peppard, 2016).

Decision-makers may use the results and terminological differentiation to address IT systems managed by BUs without the stigma that is associated with the term Shadow IT. They can use arguments related to the discussed involvement in organizational IT management (overtness) and IT task responsibility to actively turn potentially existing Shadow IT into Business-managed IT and even foster IT activities in the business for innovation in a controlled and monitored environment. Regarding implications for researchers, this paper opens a broader field of discussion on governing IT in an organization by involving BUs in IT tasks. It contributes to going beyond the primarily negative connotation of Shadow IT and complements the value-laden terminology by a vocabulary that values potentially innovative developments by business entities more adequately. Researchers may use the introduced differentiation between Business-managed and Shadow IT to classify phenomena they observe and construct theories with a wider scope.

Three conditions limit the generalizability of the perspective we have presented. First, we focused our attention on four borderline cases of Business-managed IT. While these cases are context-specific in their details, we see them as representatives for four typical manifestations of Business-managed IT. Further and more diverse cases may, however, enhance the informative value of the presented concept and the underlying dimensions. Second, we tried to circumvent potential biases stemming from the fact that the individual studies were conducted by different researchers at different times, but they cannot be completely ruled out. Third, a drawback of the case vignette methodology as used in this study is that it is useful to identify and refine concepts and relations rather than test them, which is earmarked for further studies.

Further work is needed to advance the field of Business-managed IT. As we only take a static view in our case examples, future research could examine the lifecycle of systems transitioning between

the dimensions described in our conceptual framework. Our framework also takes a simplified view on organizational structures (central and decentral), while in practice more complex forms exist (Winkler, 2013; Winkler & Brown, 2014). Moreover, a more granular perspective on the job level could be taken to identify which (IT) roles are hold by employees in Business-managed IT. Future research could address this in more detail and consider hierarchical aspects. Besides, the question arises how Business-managed IT and new ways of interdisciplinary collaboration relate to other IT management concepts regarding sourcing, building, and delivering information systems – including newer management approaches, such as agile development or colocation. Furthermore, the term Business-managed IT should be discussed in the light of emerging IS governance trends, such as "digital business units" and "IT-managed business", which can be observed at successful technology firms, for example, Zalando or Spotify. Researchers could furthermore attempt to determine the success factors and conditions required for Business-managed IT. In addition, a longitudinal study could indicate if an increasing shift of IT tasks to BUs represents a deliberate organizational design choice or if it is a gradually emergent phenomenon.

REFERENCES

Alter, S. (2014). Theory of Workarounds. *Communications of the Association for Information Systems*, *34*(1), 1041–1066. doi: 10.17705/1CAIS.03455

Andriole, S. J. (2015). Who owns IT? *Communications of the Association for Information Systems*, *58*(3), 50–57.

Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., . . . Thomas, D. (2001). Manifesto for Agile Software Development. Retrieved from http://agilemanifesto.org/

Behrens, S. (2009). Shadow Systems: The Good, The Bad and The Ugly. *Communications of the Association for Information Systems*, *52*(2), 124–129.

Beimborn, D., & Palitza, M. (2013). Enterprise App Stores for Mobile Applications: Development of a Benefits Framework. In *Proceedings of the 19th Americas Conference on Information Systems* (pp. 1–11).

Blichfeldt, B. S., & Eskerod, P. (2008). Project Portfolio Management: There's more to it than what Management Enacts. *International Journal of Project Management*, *26*(4), 357–365. doi:10.1016/j.ijproman.2007.06.004

Boynton, A. C., Zmud, R. W., & Jacobs, G. C. (1994). The Influence of IT Management Practice on IT Use in Large Organizations. *Management Information Systems Quarterly*, *18*(3), 299. doi:10.2307/249620

Brown, C. V., & Magill, S. L. (1994). Alignment of the IS Functions with the Enterprise: Toward a Model of Antecedents. *Management Information Systems Quarterly*, *18*(4), 371–403. doi:10.2307/249521

Buchwald, A., Urbach, N., & Ahlemann, F. (2014a). Business value through controlled IT: Toward an integrated model of IT governance success and its impact. *Journal of Information Technology*, *29*(2), 128–147. doi:10.1057/jit.2014.3

Buchwald, A., Urbach, N., & Ahlemann, F. (2014b). Understanding the Organizational Antecedents of Bottom-up Un-enacted-Projects. In *Proceedings of the 22nd European Conference on Information Systems* (pp. 1–16).

Bygstad, B. (2017). Generative innovation: A comparison of lightweight and heavyweight IT. *Journal of Information Technology*, *32*(2), 180–193. doi:10.1057/jit.2016.15

Capgemini. (2016). IT-Trends-Studie 2016. Retrieved from https://www.capgemini.com/de-de/resources/it-trends-studie-2016/

Chow, T., & Cao, D.-B. (2008). A survey study of critical success factors in agile software projects. *Journal of Systems and Software*, *81*(6), 961–971. doi:10.1016/j.jss.2007.08.020

Chua, C. E. H., & Storey, V. C. (2016). Bottom-up enterprise information systems. *Communications of the Association for Information Systems*, *60*(1), 66–72.

Chua, C. E. H., Storey, V. C., & Chen, L. (2014). Central IT or Shadow IT? Factors Shaping Users' Decision to Go Rogue with IT. In *Proceedings of the 35th International Conference on Information Systems* (pp. 1–14).

Daniel, E. M., Ward, J. M., & Franken, A. (2014). A Dynamic Capabilities Perspective of IS Project Portfolio Management. *The Journal of Strategic Information Systems*, *23*(2), 95–111. doi:10.1016/j.jsis.2014.03.001

Davison, R. M., Ou, C. X. J., & Chang, Y. (2018). Subverting Organisational IS Policy with Feral Systems: A Case in China. *Industrial Management & Data Systems*, *118*(3), 570–588. doi:10.1108/IMDS-04-2017-0153

Dittes, S., Urbach, N., Ahlemann, F., Smolnik, S., & Müller, T. (2015). Why Don't You Stick to Them? Understanding Factors Influencing and Counter-Measures to Combat Deviant Behavior Towards Organizational IT Standards. In O. Thomas & F. Teuteberg (Eds.), *Proceedings of the 12. Internationale Tagung Wirtschaftsinformatik: Smart Enterprise Engineering* (pp. 1–15).

Fernandez, E. B., Yoshioka, N., & Washizaki, H. (2015). Patterns for Security and Privacy in Cloud Ecosystems. In *2015 IEEE 2nd Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)* (pp. 13–18). Ottawa, Canada: IEEE. doi:10.1109/ESPRE.2015.7330162

Ferneley, E. H. (2007). Covert End User Development: A Study of Success. *Journal of Organizational and End User Computing*, *19*(1), 62–71. doi:10.4018/joeuc.2007010104

Fürstenau, D., & Rothe, H. (2014). Shadow IT Systemes: Discerning the Good and the Evil. In *Proceedings of the 22nd European Conference on Information Systems* (pp. 1–14).

Fürstenau, D., Rothe, H., & Sandner, M. (2017). Shadow Systems, Risk, and Shifting Power Relations in Organizations. *Communications of the Association for Information Systems*, *41*, 43–61. doi:10.17705/1CAIS.04103

Fürstenau, D., Sandner, M., & Anapliotis, D. (2016). Why do Shadow Sytems Fail? An Expert Study on Determinants of Discontinuation. In *Proceedings of the 24th European Conference on Information Systems* (pp. 1–16).

Gartner. (2016). Coming to Terms with Business Unit IT to Prepare for Digital Business. Retrieved from https://www.gaartner.com/doc/3288932/coming-terms-business-unit-it

Gartner. (2017). Make the Best of Shadow IT. Retrieved from https://www.gartner.com/smarterwithgartner/make-the-best-of-shadow-it/

Gozman, D., & Willcocks, L. P. (2015). Crocodiles in the Regulatory Swamp: Navigating the Dangers of Outsourcing, SaaS and Shadow IT. In *Proceedings of the 36th International Conference on Information Systems* (pp. 1–20).

Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). IT Consumerization and the Transformation of IT Governance. *Management Information Systems Quarterly*, *42*(4), 1225–1253.

Györy, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the Shadows: IT Governance Approaches to User-driven innovation. In *Proceedings of the 20th European Conference on Information Systems* (pp. 1–12).

Haag, S. (2015). Appearance of Dark Clouds? – An Empirical Analysis of Users' Shadow Sourcing of Cloud Services. In O. Thomas & F. Teuteberg (Eds.), *Proceedings of the 12. Internationale Tagung Wirtschaftsinformatik: Smart Enterprise Engineering* (pp. 1438–1452).

Haag, S., & Eckhardt, A. (2015). Justifying Shadow IT Usage. In *Proceedings of the 19th Pacific Asia Conference on Information Systems* (pp. 1–11).

Haag, S., & Eckhardt, A. (2017). Shadow IT. *Business & Information Systems Engineering*, *59*(6), 469–473. doi:10.1007/s12599-017-0497-x

Haag, S., Eckhardt, A., & Bozoyan, C. (2015). Are Shadow System Users the Better IS Users? – Insights of a Lab Experiment. In *Proceedings of the 36th International Conference on Information Systems* (pp. 1–20).

Hetzenecker, J., Sprenger, S., Kammerer, S., & Amberg, M. (2012). The Unperceived Boon and Bane of Cloud Computing: End-User Computing vs. Integration. In *Proceedings of the 18th Americas Conference on Information Systems* (pp. 1–9).

Huber, M., Zimmermann, S., Rentrop, C., & Felden, C. (2017). Integration of Shadow IT Systems with Enterprise Systems - A Literature Review. In *Proceedings of the 21st Pacific Asia Conference on Information Systems* (pp. 1–12).

Huuskonen, S., & Vakkari, P. (2013). "I Did It My Way": Social workers as secondary designers of a client information system. *Information Processing & Management*, *49*(1), 380–391. doi:10.1016/j.ipm.2012.05.003

Kent, S., Houghton, L., & Kerr, D. V. (2013). Affective Events Theory, Institutional Theory and feral Systems: How do they all Fit? In M. Grimmer & R. Hecker (Eds.), Proceedings of the 27th Australian and New Zealand Academy of Management Conference.

Khalil, S., Winkler, T. J., & Xiao, X. (2017). Two Tales of Technology: Business and IT Managers' Technological Frames Related to Cloud Computing. In *Proceedings of the 38th International Conference on Information Systems* (pp. 1–20).

Klotz, S., Kopper, A., Westner, S., & Strahringer, S. (2018). Causing Factors, Outcomes, and Governance of Shadow IT and Business-managed IT: A State-of-the-Art Literature Analysis. Manuscript submitted for publication

Köffer, S., Ortbach, K., Junglas, I., Niehaves, B., & Harris, J. (2015). Innovation Through BYOD? The Influence of IT Consumerization on Individual IT Innovation Behavior. *Business & Information Systems Engineering*, *57*(6), 363–375. doi:10.1007/s12599-015-0387-z

Kopper, A. (2017). Perceptions of IT Managers on Shadow IT. In *Proceedings of the 23rd Americas Conference on Information Systems* (pp. 1–10).

Kopper, A., & Westner, M. (2016a). Deriving a Framework for Causes, Consequences, and Governance of Shadow IT from Literature. In V. Nissen, D. Stelzer, S. Straßburger, & D. Fischer (Eds.), *Proceedings of the Multikonferenz Wirtschaftsinformatik* (pp. 1687–1698).

Kopper, A., & Westner, M. (2016b). Towards a Taxonomy for Shadow IT. In *Proceedings of the 22nd Americas Conference on Information Systems* (pp. 1–10).

Kopper, A., Westner, M., & Strahringer, S. (2017). Kontrollierte Nutzung von Schatten-IT. *HMD Praxis Der Wirtschaftsinformatik*, *54*(1), 97–110. doi:10.1365/s40702-016-0286-x

Kretzer, M., & Maedche, A. (2014). Generativity of Business Intelligence Platforms: A Research Agenda Guided by Lessons from Shadow IT. In D. Kundisch, L. Suhl, & L. Beckmann (Eds.), *Proceedings of the Multikonferenz Wirtschaftsinformatik* (pp. 208–220). Paderborn.

Levy, Y., & Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science: the International Journal of an Emerging Transdiscipline*, *9*, 181–212. doi:10.28945/479

Lund-Jensen, R., Azaria, C., Permien, F. H., Sawari, J., & Bækgaard, L. (2016). Feral Information Systems, Shadow Systems, and Workarounds: A Drift in IS Terminology. *Procedia Computer Science*, *100*, 1056–1063. doi:10.1016/j.procs.2016.09.281

McIvor, R. (2009). How the Transaction Cost and Resource-Based Theories of the Firm Inform Outsourcing Evaluation. *Journal of Operations Management*, *27*(1), 45–63. doi:10.1016/j.jom.2008.03.004

Myers, N., Starliper, M. W., Summers, S. L., & Wood, D. A. (2017). The Impact of Shadow IT Systems on Perceived Information Credibility and Managerial Decision Making. *Accounting Horizons*, *31*(3), 105–123. doi:10.2308/acch-51737

Ortbach, K. (2015). Unraveling the Effect of Personal Innovativeness on Bring-Your-Own-Device (BYOD) Intention: The Role of Perceptions Towards Enterprise-Provided and Privately-Owned Technologies. In *Proceedings of the 23rd European Conference on Information Systems* (pp. 1–17).

Panko, R. R., & Port, D. N. (2012). End User Computing: The Dark Matter (and Dark Energy) of Corporate IT. In *Proceedings of the 45th Hawaii International Conference on System Sciences* (pp. 4603–4612). IEEE. doi:10.1109/HICSS.2012.244

Peppard, J. (2016). Rethinking the concept of the IS organization. *Information Systems Journal*, *28*(1), 76–103. doi:10.1111/isj.12122

Power, M. (2007). *Organized Uncertainty: Designing a World of Risk Management* (1st ed.). New York, USA: Oxford University Press.

Rentrop, C., & Zimmermann, S. (2012a). Shadow IT Evaluation Model. In *Proceedings of the Federated Conference on Computer Science and Information Systems* (pp. 1023–1027). Piscataway, NJ: IEEE.

Rentrop, C., & Zimmermann, S. (2012b). Shadow IT: Management and Control of unofficial IT. In J. Lloret Mauri, G. Martínez, L. Berntzen, & Å. Smedberg (Eds.), *Proceedings of the 6th International Conference on Digital Society* (98–102). Wilmington, USA: IARIA.

Röder, N., Wiesche, M., & Schermann, M. (2014). A Situational Perspective on Workarounds in IT-enabled Business Processes: A Multiple Case Study. In *Proceedings of the 22nd European Conference on Information Systems* (pp. 0–15).

Seawright, J., & Gerring, J. (2008). Case selection techniques in case study research: A menu of qualitative and quantitative options. *Political Research Quarterly*, *61*(2), 294–308. doi:10.1177/1065912907313077

Sedera, D., Lokuge, S., Grover, V., Sarker, S., & Sarker, S. (2016). Innovating with enterprise systems and digital platforms: A contingent resource-based theory view. *Information & Management*, *53*(3), 366–379. doi:10.1016/j.im.2016.01.001

Silic, M., & Back, A. (2014). Shadow IT – A view from behind the curtain. *Computers & Security*, *45*, 274–283. doi:10.1016/j.cose.2014.06.007

Silic, M., Silic, D., & Oblakovic, G. (2016). Influence of Shadow IT on Innovation in Organizations. *Complex Systems Informatics and Modeling Quarterly*. (8), 68–80.

Singh, H. (2015). Emergence and Consequences of Drift in Organizational Information Systems. In *Proceedings of the 19th Pacific Asia Conference on Information Systems* (pp. 1–15).

Spierings, A., Kerr, D. V., & Houghton, L. (2012). What Drives the End User to Build a Feral Information System? In *Proceedings of the 23rd Australasian Conference on Information Systems* (pp. 1–10).

Spierings, A., Kerr, D. V., & Houghton, L. (2017). Issues that support the creation of ICT workarounds: Towards a theoretical understanding of feral information systems. *Information Systems Journal*, *27*(6), 775–794. doi:10.1111/isj.12123

Tambo, T., & Bækgaard, L. (2013). Dilemmas in Enterprise Architecture Research and Practice from a Perspective of Feral Information Systems. In *Proceedings of the 17th IEEE International Enterprise Distributed Object Computing Conference Workshops* (pp. 289–295). IEEE. doi:10.1109/EDOCW.2013.38

TechTarget. (2014). What is embedded IT? Retrieved from http://searchcio.techtarget.com/definition/embedded-IT

TechTarget. (2016). What is citizen development? Retrieved from http://searchsalesforce.techtarget.com/definition/citizen-development

Walterbusch, M., Fietz, A., & Teuteberg, F. (2017). Missing cloud security awareness: Investigating risk exposure in shadow IT. *Journal of Enterprise Information Management*, *30*(4), 644–665. doi:10.1108/JEIM-07-2015-0066

Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, USA: Harvard Business School Press.

Winkler, T. J. (2013). IT Governance Mechanisms and Administration/IT Alignment in the Public Sector: A Conceptual Model and Case Validation. In R. Alt & B. Franczyk (Eds.), *Proceedings of the 11. Internationale Tagung Wirtschaftsinformatik* (pp. 831–845).

Winkler, T. J., & Brown, C. V. (2013). Horizontal Allocation of Decision Rights for On-Premise Applications and Software-as-a-Service. *Journal of Management Information Systems*, *30*(3), 13–48. doi:10.2753/MIS0742-1222300302

Winkler, T. J., & Brown, C. V. (2014). Organizing and Configuring the IT Function. In A. Tucker, T. Gonzalez, H. Topi, & J. Diaz-Herrera (Eds.), *Computing Handbook: Information Systems and Information Technology* (3rd ed., Vol. 2, pp. 1–14). Boca Raton, FL: C R C Press LLC.

Winter, S., Berente, N., Howison, J., & Butler, B. (2014). Beyond the organizational 'container': Conceptualizing 21st century sociotechnical work. *Information and Organization*, *24*(4), 250–269. doi:10.1016/j.infoandorg.2014.10.003

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

Zainuddin, E. (2012). Secretly SaaS-ing: Stealth Adoption of Software-as-a-Service from the Embeddedness Perspective. In *Proceedings of the 33rd International Conference on Information Systems* (pp. 1–10).

Zimmermann, S., & Rentrop, C. (2012). Schatten-IT. *HMD Praxis Der Wirtschaftsinformatik*, *49*(6), 60–68. doi:10.1007/BF03340758

Zimmermann, S., & Rentrop, C. (2014). On the Emergence of Shadow IT - A Transaction Cost-based Approach. In *Proceedings of the 22nd European Conference on Information Systems* (pp. 1–17).

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 20th Americas Conference on Information Systems* (pp. 1–12).

Zimmermann, S., Rentrop, C., & Felden, C. (2016). Governing Identified Shadow IT by Allocating IT Task Responsibilities. In *Proceedings of the 22nd Americas Conference on Information Systems* (pp. 1–10).

Zimmermann, S., Rentrop, C., & Felden, C. (2017). A Multiple Case Study on the Nature and Management of Shadow Information Technology. *Journal of Information Systems*, *31*(1), 79–101. doi:10.2308/isys-51579