Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

SHADOW IT AND BUSINESS-MANAGED IT: PRACTITIONER PERCEPTIONS AND THEIR COMPARISON TO LITERATURE

ANDREAS KOPPER
TU DRESDEN
andreas.kopper@mailbox.tu-dresden.de

STEFAN KLOTZ
TU DRESDEN
stefan.klotz1@mailbox.tu-dresden.de

MARKUS WESTNER
OTH REGENSBURG
markus.westner@oth-regensburg.de

SUSANNE STRAHRINGER
TU DRESDEN
susanne.strahringer@tu-dresden.de

ABSTRACT

Two concepts describe the autonomous deployment of IT by business entities: Shadow IT and Business-managed IT. Shadow IT is deployed covertly, that is, software, hardware, or IT services created/procured or managed by business entities without alignment with the IT organization. In contrast, Business-managed IT describes the overt deployment of IT, that is, in alignment with the IT organization or in a split responsibility model. The purpose of this paper is to extend the conceptual understanding of Shadow IT and Business-managed IT, comparing the perceptions of 29 CIOs and senior IT managers with the results of a systematic literature review. By doing so, this paper presents a structured and comprehensive view of causing factors, outcomes, and governance of Shadow IT and Business-managed IT in practice. A comparison of academic literature and practitioner perceptions reveals the limitations and gaps of the current research and highlights avenues for future research. The authors find three category-spanning themes occurring as causing factors, outcomes, and—as part of governance measures—factors to improve the IT organization: (1) (Poor) business-IT alignment (2) (lack of) agility, and (3) (lack of) policies. This study is innovative with its comprehensive qualitative interview data that the authors compare to the existing literature. Therefore, the paper brings together theoretical and practical insights into Shadow IT and Business-managed IT, which should aid practitioners and scholars in decision making and future research.

Keywords: Shadow IT, Business-managed IT, IT governance, agility, business-IT alignment

INTRODUCTION

Shadow IT describes the autonomous development/procurement or management of software, hardware, or IT services (incl. SaaS, PaaS, IaaS) by business units (BUs), that is, individual users, business workgroups, departments, or divisions, without alignment with the IT organization (Kopper et al. [56]; Zimmermann and Rentrop [109]). With the term IT organization, we refer to internal IT organizations, for example, company-internal IT departments (Klotz et al. [51]). Shadow IT is a widespread phenomenon in practice (Kopper [54]). Segal [88], for example, finds that 80% of employees use software unapproved by the IT organization, and Gartner [33] estimates that 38% of technology purchases are managed, defined, and controlled by business leaders. However, CIOs vastly underestimate the true extent of Shadow IT usage in companies (Corbin [21]).

As defined, Shadow IT manifestations are covert (Ferneley [26]) from the organizational IT management. This changes as soon as Shadow IT instances become visible (Klotz et al. [51]), for example, due to monitoring (Buchwald et al. [15]). Kopper et al. [56] have introduced a conceptual model to differentiate between covert (hidden) Shadow IT and overt (visible) Business-managed IT. Accordingly, Shadow IT and Business-managed IT share the characteristic that IT task responsibility usually lies with the BU (except for Shadow IT within the IT organization itself). In contrast to Shadow IT, Business-managed IT is (overtly) part of the organizational IT management (Kopper et al. [55]; Kopper et al. [56]). Therefore, Business-managed IT is defined as the autonomous and overt development/procurement or management of software, hardware, or IT services (incl. SaaS, PaaS, IaaS) by BUs either in alignment with the IT organization or in a split responsibility model (Kopper et al. [55]; Kopper et al. [56]).

The differentiation between Shadow IT and Business-managed IT yields implications for governance practices as the overtness of Business-managed IT instances enables further governance mechanisms (Klotz et al. [51]). However, this differentiation is currently not made in discussions around the phenomena (Kopper et al. [56]). Klotz et al. [51] have addressed this research gap with a review of the academic literature of the two phenomena and discuss the differentiation of 34 research themes for Shadow IT and Business-managed IT. However, the lens of practitioners on the two phenomena is still missing in current literature, and there is a potential gap between academic research and practitioner perceptions, as discovered in several IS research streams (Marrone and Hammerle [68]; Ramiller and Pentland [81]). Hence, we aim to contribute to a more nuanced understanding of and a discussion around Shadow IT and Business-managed IT from an integrated perspective that includes the scholarly as well as the practitioner lens. By doing so, we build a basis for discussions and develop a research agenda (Marrone and Hammerle [68]). Therefore, we pose the following research question: *Which practitioner perceptions exist concerning Shadow IT and Business-managed IT, and how do these relate to the research themes in existing academic literature?*

Our results are relevant for both scholars and practitioners. Researchers can use them to get a better conceptual understanding of Shadow IT and Business-managed IT and to focus their research on the identified research gaps, for example, on research themes with high practitioner interest but low coverage in academic literature. Building on the framework and the identified themes, practitioners can gain a broader understanding of the two phenomena. They can make better strategic decisions about IT governance and the distribution of IT task responsibilities.

This paper is structured as follows: First, we provide an overview of the literature building on a framework of causing factors, outcomes, and governance. By doing so, we also conceptualize the phenomena of interest. After that, we give a brief methodological overview. Then, we present the results of the practitioner interviews in an extended framework of causing factors, outcomes, and governance and detail each of the themes. Subsequently, we discuss the differences between academic and practitioner perceptions. Finally, we conclude with a summary of the paper, remarks on its contributions, limitations, and avenues for future research.

CONCEPTUALIZATION AND RELATED WORK

The existing research on Shadow IT and Business-managed IT can be structured in a framework of causing factors, outcomes, and governance (Haag and Eckhardt [40]; Klotz et al. [51]; Kopper and Westner [57]). Within this paper, we build on the rigorous (vom Brocke et al. [100]) and systematic (Webster and Watson [104]) literature review by Klotz et al. [51] who reviewed 107 literature items on Shadow IT and Business-managed IT and their resulting framework. Figure 1 illustrates the framework structure (see Figure 3 for the full and extended framework). For *causing factors*, we distinguish the subcategories enablers, motivators, and missing barriers. Shadow IT and Business-managed IT is enabled by user-friendly IT solutions (Ferneley [26]) and the resulting simplified technical accessibility as well as the increasing

IT user competence in business entities (Ortbach et al. [75]; Spierings et al. [95]; Spierings et al. [96]). Furthermore, the deployment or procurement of Shadow IT and Business-managed IT is motivated by non-alignment of the IT organization and BUs (Khalil et al. [49]), shortcomings of existing IT systems (Fürstenau et al. [32]), or the motivation of employees and the behavior of peers (Haag and Eckhardt [39]). Moreover, lacking restrictions (Silic and Back [90]) and awareness (Dittes et al. [24]) can be missing barriers to prevent Shadow IT usage.

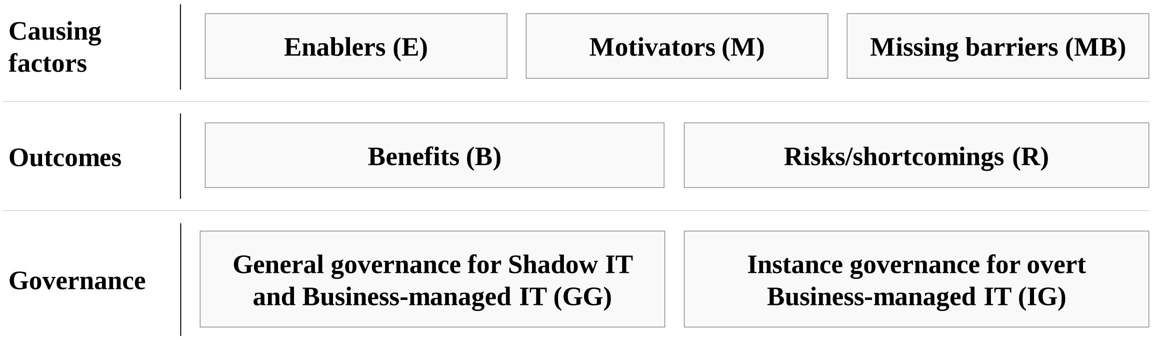

Causing factors
Enablers (E)
Motivators (M)
Missing barriers (MB)
Outcomes
Benefits (B)
Risks/shortcomings (R)
Governance
General governance for Shadow IT and Business-managed IT (GG)
Instance governance for overt Business-managed IT (IG)

Figure 1: Framework Structure for Causing Factors, Outcomes, and Governance of Shadow IT and Business-managed IT based on Klotz et al. [51]

Because Shadow IT and Business-managed IT can have positive and negative *outcomes*, we differentiate the benefits and risks/shortcomings of Shadow IT and Business-managed IT. On the one hand, Shadow IT and Business-managed IT are generally associated with benefits such as increased productivity (Ahuja and Gallupe [1]), innovation (Fürstenau and Rothe [28]), or agility (Khalil et al. [49]). On the other hand, literature has also emphasized risks/shortcomings which are more apparent for Shadow IT, as the higher transparency of overt Business-managed IT enables better mitigation of these in comparison to Shadow IT (Kopper et al. [55]; Kopper et al. [56]). In brief, researchers commonly highlight security risks (Haag and Eckhardt [38]), integration issues (Kopper et al. [58]), or inefficiencies and loss of synergies (Györy et al. [35]) as potential adverse effects. Khalil et al. [49] noticed a different perception of Shadow IT in the form of cloud services between business and IT managers: "While the business group particularly emphasizes the benefits generated by cloud technology (total frequency of 19), the IT managers group has less focus on benefits (freq. of 9)" (Khalil et al. [49, p. 8]). However, "IT managers put more emphasis on the threats related to cloud computing (total freq. of 25) than the business managers (total freq. of 6)" (Khalil et al. [49, p. 9]).

The overtness of IT instances fundamentally affects the *governance* of Shadow IT and Business-managed IT (Klotz et al. [51]). That is, general governance measures exist for Shadow IT and Business-managed IT, which can be applied regardless of their "visibility" (overt or covert); however, for overt Business-managed IT instances, also more specific governance measures exist. General governance measures include policies regulating IT usage in BUs (Behrens [6]), increasing awareness, for example, through training (Haag [36]), the resolving of IT gaps (Walterbusch et al. [101]), or the monitoring and identification of instances (Röder et al. [86]). For (overt) Business-managed IT instances, more specific governance measures exist. That is, transparent Business-managed IT instances can be categorized, and two decision points for their governance exist (Klotz et al. [51]). The first decision to be made is decommission (Kopper [54]) or continuation. If instances are continued, the second decision point determines the governance allocation. The governance responsibility can be allocated to either the IT organization (Zimmermann et al. [113]), the BU (Andriole [3]), or split in a shared responsibility model (Zimmermann et al. [112]). Another characterization of the second decision point could be to generally enable the creation of (future) Business-managed IT by defining general governance models for it (Klotz et al. [51]).

Only a few scholars have studied Shadow IT and Business-managed IT in a category-spanning way from a practitioner perspective, that is, across causing factors, outcomes, and governance (Klotz [50]). Khalil et al. [49] interviewed 20 business and IT professionals in 2015-2016 and have identified technological frames for benefits, threats, and governance and control. As benefit frames, they have found economics, agility, performance, ubiquity, and scalability. As threat frames, they have determined security, compliance, reversibility, and dependency. They have also stated power, agility, tailored solutions, and restrictions for business units as governance and control frames. In their interviews, business managers emphasized the benefits of cloud computing and put less focus on risks, while for IT managers, it was the other way around (Khalil et al. [49]).

Walterbusch et al. [102] gathered data from a survey with students and university employees, conducted a vignette study, and interviewed ten experts to complement a literature review from 2013. They have identified five potential risks for Shadow IT through the expert interviews: Stolen data/corporate espionage, malware/spyware, missing backup(s), data location, and loss of compatibility/inside knowledge. Based on these risks, they discuss potential governance measures to restrict Shadow IT: Closing specific network ports, restricting administrative rights, blacklisting and whitelisting, blocking websites or usage of thin clients, and awareness creation in employees. Walterbusch et al. [102] structured their findings using a morphological box along with eight criteria, and they have introduced belief-action-outcome models for employees and employers.

In an earlier literature review (Klotz et al. [51]), we have determined that only a few existing studies focus on exploring the field of Shadow IT based on practitioner interviews. Moreover, these studies do not differentiate Shadow IT and Business-managed IT. Consequently, previous research does not provide an integrated framework of practitioner perceptions and existing literature to structure the research field. Hence, an integrated perspective of the academic and practitioner perceptions on Shadow IT and Business-managed IT would be beneficial to structure the research field.

METHODOLOGY

To create an integrated perspective of the research stream, we selected interviews to collect data on cases of Shadow IT and Business-managed IT. Interviews are appropriate to answer our explorative research question because Shadow IT and Business-managed IT are complex, many-faceted topics that require understanding and mutual correspondence of the underlying principles and terminologies (Benbasat et al. [9]; Pan and Tan [77]; Yin [106]). Moreover, Shadow IT has a mostly negative connotation (Kopper [54]) and is, thus, a highly sensitive topic. In order to build a high degree of trust between the interview partners to talk about Shadow IT, we aimed for trust-building from a social and legal perspective using personal recommendations. We submitted non-disclosure agreements in advance of the interviews. Therefore, all data and results are anonymized. Overall, we conducted 29 interviews with executive/senior IT managers or business managers with a close link to IT (P01-P29). Table 1 provides an overview of the interview participants. The number of interviews ensured coverage of a broad company spectrum regarding industries, organizational setups, and sizes. That is, we focused on medium and large companies from different industries because they usually have distinctive organizational structures, for example, a separate IT organization. The participant selection concentrated on German-speaking countries, that is, the DACH area (Germany, Austria, Switzerland), to reduce linguistic misunderstandings and cultural differences. After a pilot interview (Yin [106]) in July 2016, the remaining interviews took place from October 2016 to June 2017. To gather descriptive company information, for example, revenue and number of IT users, we sent a written survey to the participants before the interview.

The interviews lasted one hour on average and were mainly conducted in the form of video or audio conferences (except for three on-site interviews). We used a semi-structured approach with open questions as described by Myers and Newman [73] and Yin [106] to allow the participants to speak freely about their perceptions and experiences. In particular, we asked open questions on (1) the context of specific Shadow IT and Business-managed IT instances, (2) the positive and negative effects of the instances, (3) the causes for the instances, and (4) organizational, technical, and general measures of the instances. We limited the predefined structure to these topics instead of following frameworks of causing factors, outcomes, and governance (such as in Figure 1) to avoid confirmation bias and allow for flexibility. During the interviews, we used improvisation and listening strategies for detailed follow-up questions (Myers and Newman [73]) to understand the organizational and technical context. We recorded and transcribed the interviews (except for P28).

To analyze the transcribed interview data, we used coding with MAXQDA (Corbin and Strauss [20]; Yin [106]). As an initial coding scheme, we applied the research framework of causing factors, outcomes, and governance for Shadow IT and Business-managed IT – introduced by Kopper and Westner [57] and adapted by Klotz et al. [51] (see Figure 3 and Figure 4) to ensure research continuity. In addition, open coding guidelines provided the basis for the identification of additional (sub)categories (Corbin and Strauss [20]). The codes were validated by the second author using random sampling.

Table 1: Characteristics of Interview Participants

Position/Role of Interview Participants	**Number of Participants**
CIO	19
Senior IT manager	5
CTO	1
CIO & CFO	1
DTO	1
CEO	1
Senior business manager	1
Total	**29**

Industries	**Number of Participants**
Health Care & Health Care Equipment	4
Commercial Services	3
Electrical & Electronic Equipment	3
Energy & Utilities	3
Financial Services	3
Information Technology	2
Insurance	2
Public Sector	2
Retail & Wholesale	2
Consumer Goods	1
Engineering Services	1
Machinery	1
Telecommunications	1
Transportation	1
Total	**29**

RESULTS

We describe the emerging themes from the interviews, along with the framework of causing factors, outcomes, and governance (Klotz et al. [51]). Figure 2 shows the coding results for each study participant, and Figure 3 summarizes the extended framework for causing factors, outcomes, and governance of Shadow IT and Business-managed IT. In the following sections, we describe each of the themes in detail.

Causing Factors

Within causing factors, we distinguish *enablers (E), motivators (M),* and *missing barriers* (MB).

Enablers (E)

E1 Technical accessibility. Literature supports the notion that decreased complexity (Zimmermann and Rentrop [108]) and increased user-friendliness (Ferneley [26]) of IT systems make it easier for BUs to autonomously deploy them (Spierings et al. [96]; Thatte et al. [99]). Especially cloud offerings (Haag and Eckhardt [40]) and end-user hardware (Davison et al. [23]; Davison and Ou [22]; Walters [103]) are highlighted as examples. However, only three participants (P01, P06, P14) (10%) explicitly mentioned this theme. P06 acknowledged that cloud services reduce the dependence of BUs on the IT organization and expected this context to increase further (Haag and Eckhardt [40]). P01 described an example where, after being unhappy with the IT organization's offer, a BU could cover a requirement by independently procuring a solution consisting of a mobile app and a cloud backend. However, P01 and P14 criticized that (1) vendors directly approach BUs and users and (2) make their systems directly accessible without having to involve the IT organization (which would otherwise allow assessing the solutions accurately).

E2 IT user competence. While not supporting the view that IT knowledge generally increases in BUs as mentioned in the literature (Ferneley [26]; Fürstenau and Rothe [28]), participants generally agree (24%) that IT-related skills allow BUs to employ or procure IT solutions independently (Chua et al. [19]). In this context, P21, for example, mentioned skilled young professionals or digital natives joining the company directly after attending university (Ahuja and Gallupe [1]; Davison et al. [23]; Rentrop and Zimmermann [82]). Others described cases of Business-managed IT that are enabled by employees with high IT skills (P06, P28) (Silic and Back [90]; Spierings et al. [95]), especially ones with relation to R&D (P16). P11 said that such "tool-affine types could be found in each BU." P08 and P15 explained that the bigger the BU, the more likely that the required resources and skills are present to develop IT systems independently.

Subcategory	ID	Theme	P01	P02	P03	P04	P05	P06	P07	P08	P09	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29
Enablers	E1	Technical accessibility	x					x								x															
	E2	IT user competence						x		x			x				x				x		x							x	
	E3	Hubris	x		x			x							x			x		x		x									x
Motivators	M1	IT organization and BU non-alignment	x		x	x	x			x		x	x		x	x	x				x		x	x				x			
	M2	IT system shortcomings					x							x											x			x			
	M3	Employee motivation/impact orientation & peer beh.	x																							x					
	M4	IT organization slowness	x	x	x	x	x	x	x	x			x	x	x	x		x		x	x				x		x			x	
	M5	Beneficial cost structure anticipation	x	x				x					x							x											
	M6	Business environment uncertainty	x						x								x	x											x	x	
	M7	Competence lack/resource scarcity in IT organization		x	x	x	x		x		x			x			x		x	x			x		x			x	x		
	M8	BU power loss		x		x	x	x														x									x
	M9	Tailored solutions	x			x	x																		x			x			
Missing barriers	MB1	Restriction lack	x		x	x	x	x			x	x			x		x		x	x	x	x	x		x						x
	MB2	Awareness lack										x																			
Benefits	B1	Productivity gain												x				x									x	x			
	B2	Innovation increase			x																									x	
	B3	Agility enhancement & flexibility increase	x	x	x	x	x	x	x				x	x	x		x	x		x	x				x	x		x	x		x
	B4	User/customer satisfaction improvement	x	x		x		x																	x						x
	B5	Collaboration enhancement											x																		
Risks / shortcomings	R1	Security risks & lacking data privacy	x	x	x	x		x	x	x		x			x		x			x	x		x		x	x	x		x	x	
	R2	Integration lack & data inconsist. & architect. insuff.	x	x	x		x	x	x		x	x	x	x	x		x	x				x							x		x
	R3	Synergy loss & inefficiency creation	x		x			x		x	x	x		x	x					x	x		x	x	x	x			x	x	x
	R4	Control loss	x	x	x		x				x			x			x											x			x
	R5	Continuity lack	x	x	x	x		x	x					x	x	x	x	x		x								x		x	
	R6	Quality issues	x		x			x		x		x	x	x	x					x		x	x	x	x						x
General governance	GG1	Policy setup	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x
	GG2	Awareness training	x											x		x							x			x					
	GG3	IT gap resolution																													
	GG3-1	More agility	x	x	x		x		x			x	x		x	x	x	x	x	x		x	x	x	x	x	x	x	x		x
	GG3-2	Better business-IT alignment	x		x	x	x		x		x	x	x	x	x	x	x	x				x			x		x	x	x	x	
	GG3-3	System modernization	x	x		x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x
	GG4	Monitoring & identification			x	x			x			x		x	x	x		x				x	x	x	x	x	x	x	x	x	x
Governance for overt instances	IG1	Instance categorization								x		x	x		x	x											x	x		x	x
	IG2	Instance decommission										x		x		x		x		x							x	x		x	x
	IG3	IT organization instance governance	x	x	x		x			x	x	x			x										x						
	IG4	IT organization & BU instance co-governance																													
	IG4-1	IT organization providing platform				x	x	x	x				x				x	x	x		x		x		x		x	x	x		x
	IG4-2	IT organization managing risk		x		x		x	x									x	x				x		x		x		x		x
	IG4-3	IT organization supporting implementation		x		x		x	x				x	x	x		x	x	x				x		x			x	x	x	x
	IG4-4	BU defining requirements/designing application				x	x	x	x				x				x	x	x		x		x		x		x				
	IG5	BU instance governance		x		x				x	x														x	x			x	x	x

Figure 2: Themes Discussed by Study Participants

E3 Hubris. An enabler not identified in literature but brought up by eight participants (28%) in a negative context is an overestimation of BUs' own IT capabilities. Some BUs are convinced that they are better than the IT organization in terms of developing solutions, despite negative results (P06, P16, P29). P18 and P20 cited as a possible explanation that some individuals in BUs believe that it is their vocation to be an IT developer. P01 stated that the self-confidence of a BU head correlates with the number of Shadow IT projects, P03 observed a certain arrogance in this context, and P13 described an example of a BU not accepting advice despite a poorly implemented project.

Motivators (M)

M1 IT organization and BU non-alignment. The interview data support (48%) the theoretical findings that a lack of business-IT alignment motivates Shadow IT and Business-managed IT (Houghton and Kerr [43]; Kerr et al. [48]; Kopper [54]; Ologeanu-Taddei et al. [74]). P01, P08, and P15 described a lack of communication of requirements and ideas (Beimborn and Palitza [8]; Silic et al. [92]) that lead to unmet user needs (Khalil et al. [49]; McCoy and Rosenbaum [69]; Singh [94]; Walterbusch et al. [102]). BUs also perceive coordination with the IT organization as too much effort and seek alternatives (P01, P03) (Buchwald and Urbach [13]; Buchwald and Urbach [14]). Previous detrimental experiences with the IT organization (Tambo and Bækgaard [98]; Zimmermann and Rentrop [109]) stem from frequent rejections of requests from BUs, for example, due to security concerns, without offering alternatives (P01, P05, P10, P21, P26). This can lead to general doubts about the abilities of the IT organization (P11, P22). In other cases, cultural aspects were identified where newer and older BUs in the organization have different attitudes towards the centralization of IT (P04, P19). The most common issue identified was that the IT organization is often only viewed as a fulfillment provider or cost center instead of a trusted partner (Silic et al. [92]; Silic and Back [90]; Zainuddin [107]) who could help to provide value from the beginning of a project (P01, P13, P14, P16, P19, P22). For example, P19 explained that "[…] it is quite hard to create [a] real partnership. [The IT organization] was [rather] always perceived by [the] business as a cost center and unnecessary evil".

M2 IT system shortcomings. Only four participants (P5, P12, P23, P26) (14%) explicitly mentioned examples of shortcomings of existing systems as a motivator for Shadow IT and Business-managed IT (Berente et al. [10]; Huuskonen and Vakkari [46]; Zimmermann et al. [113]). Most of the cases deal with the creation of new systems that do not aim to replace an old, inadequate one. However, P12 (similarly P23) described an area where formal systems did not provide enough flexibility, and users, therefore, created other solutions (Boudreau and Robey [12]). P05 mentioned an ERP system which did not provide the functionality required by the users, and they thus built workaround systems (Lund-Jensen et al. [62]; Lyytinen and Newman [63]; Silva and Fulk [93]). Similarly, users build macros to automate inefficient workflows in existing systems (P26). However, no participant talked about malfunctioning**,** officially provided IT solutions (Hetzenecker et al. [42]; Koopman and Hoffman [53]), which, for example, hold incorrect data (Azad and King [4]; Behrens [6]; Bob-Jones et al. [11]).

M3 Employee motivation/impact orientation & peer behavior. Two participants (P01, P24) (7%) highlighted employee motivation as a significant factor for Shadow IT and Business-managed IT (Buchwald and Urbach [13]; Haag et al. [41]; Haag and Eckhardt [37]). P24 mentioned highly motivated employees who built small applications in their overtime to increase individual task or job performance (Haag [36]; Mallmann and Maçada [64]; Schalow et al. [87]). In a negative context, P01 described an "over-motivated" BU head who wanted to support his business with a comprehensive solution but accepted potential risks by not aligning with the IT organization (Röder et al. [85]; Silic et al. [91]). Not mentioned as an influencing factor was the behavior of peers (Buchwald et al. [15]; Mallmann and Maçada [65]; Spierings et al. [96]).

M4 IT organization slowness. The most prominent motivating factor in the interviews (62%) was that BUs perceive the IT organization as being too slow in fulfilling their requirements (P01, P02, P07, P11, P12, P18, P19, P23, P25). They also expect more agility, flexibility (Fürstenau et al. [32]; Haag and Eckhardt [39]; Khalil et al. [49]), and a more iterative approach to development (P01, P03, P18, P28). P18 explained that "[the BUs] want things to be done faster, they do not like […] to wait, they would like it to be more iterative". Slow responsiveness to requests (P05, P19) (Behrens and Sedera [7]; Jones et al. [47]; Singh [94]), bureaucratic processes (P18), and long planning periods (P08) were mentioned as examples. In some cases, a disadvantageous request prioritization from the view of the BU leads to long waiting times (P08, P12) (Behrens [6]; Chua et al. [19]). Participants also recognized that alignment with the IT organization leads to more coordination efforts in comparison to efficiently and directly working close to the problem being solved or close to the user/customer (P02, P04, P06, P14). P02, for example, highlighted that "centralization always means slowing down." Centrally dictated or checked guidelines, for example, in terms of documentation, security, or testing, are therefore sometimes perceived as unnecessary overhead (P01, P06). The participants also identified large, inflexible systems (ERP or CRM) or legacy infrastructure as a cause for not being able to implement requirements faster (P11, P13, P18, P19, P25). In literature, these aspects are subsumed under long development times (Chua and Storey [18]; Kopper [54]; Zimmermann et al. [110]) and lengthy procurement processes (Walters [103])).

M5 Beneficial cost structure anticipation. Six participants (17%) identified costs as a factor for BUs seeking alternatives for working with the IT organization (Györy et al. [35]; Kopper [54]; Zimmermann and Rentrop [109]). The BUs may perceive the services of the IT organization as too expensive (P01), for example, if they only associate it with large ERP implementations (P11). Consequently, they pick cheaper alternatives (P02), for example, external system integrators with more competitive hourly rates (P01). Because costs correlate with implementation time (M4), BUs may similarly perceive integration with other systems or guidelines about documentation, security, or testing as an unnecessary cost overhead (P01, P06) (Spierings et al. [96]; Tambo and Bækgaard [98]). P18 mentioned an example where users do not want to deal with the process of getting approval for IT costs and therefore implement their solutions.

M6 Business environment uncertainty. Supported by 21% of participants, P07, for example, explained that Shadow IT emerges in cases where BUs are not yet able to formulate their requirements clearly and need to figure them out in an agile way. Business-managed IT is also motivated by the uncertainty around new topics (P15) which require flexibility (Zimmermann et al. [113]), especially when diversifying the product portfolio (P01) (Fürstenau et al. [31]; Fürstenau et al. [29]), for example through internal startup accelerators (P27, P28) or proof-of-concept projects (P16).

M7 Competence lack/resource scarcity in IT organization. A smaller theme in literature but mentioned by almost half of all participants (48%) is that the IT organization has limited resources and is realistically not able to fulfill all requests (P02, P03, P04, P05, P09, P18) (Fürstenau et al. [32]; Kopper et al. [56]). Therefore, requests have to be prioritized, and some of them eventually are dropped, which leads to BUs either covertly looking for alternatives or IT organizations deliberately handing over responsibilities (P07, P12, P18, P23, P26). Similarly, it seems beneficial to engage in Business-managed IT if the IT organization does not have the necessary (business process) know-how for a request (P15, P17, P21, P27) (Fürstenau et al. [32]; Zimmermann and Rentrop [109]).

M8 BU power loss. As in literature, the loss of power is a less prominent (21%) motivating factor for Shadow IT and Business-managed IT (Fürstenau et al. [31]; Fürstenau et al. [29]). The BUs may generally favor more control and independence over the implementation of IT systems (P02, P29). Individuals can also use IT systems to create dependencies and secure their job (P04, P06) or use separate systems to avoid transparency and sharing data with the rest of the organization (P05, P20).

M9 Tailored solutions. Awareness emerged in the interviews (by 17% of the participants) that BUs may prefer (familiar) solutions that precisely fit their requirements and do not want to make any compromises for the sake of organization-wide standardization (P01, P04, P05, P23). This can also apply to projects when a BU prefers to work with an external solution provider who precisely fulfills all requests instead of having to adhere to organizational standards when working with the IT organization (P01). However, at least for highly specific requirements, Business-managed IT can be a viable option (P04, P26). This theme was not identified in the literature.

Missing Barriers (MB)

MB1 Restriction lack. A lack of restrictions was brought up by 55% of participants. Several of them (P03, P09, P10, P19, P21, P23) said that they do not yet have a clear, formally defined policy for Shadow IT and Business-managed IT (Fürstenau et al. [31]; Silic and Back [90]; Walterbusch et al. [102]). While for some areas, the split of IT task responsibilities is at least implicitly clear, for others, the boundaries are an ongoing source of conflict (P15) or difficult to determine, especially on a detailed technical level (P17, P29). Another contributing factor is the ability of BUs to use internal business budgets for IT projects (P01, P05, P06, P18) (Khalil et al. [49]) or that BUs could get CEO approval for circumventing the IT organization (P21). Even for areas where policies are defined, there may be no consequences for circumventing them (P03, P05, P18, P20), showing that prohibitions might have limited effects (Rentrop et al. [84]).

MB2 Awareness lack. In contrast to the literature, only one participant (P10) (3%) mentioned a lack of awareness of existing policies as a potential cause for Shadow IT, especially around institutionalized shadow systems. This may relate to the previously mentioned fact that policies themselves are frequently undefined or unclear (Beimborn and Palitza [8]; Dittes et al. [24]; Mokosch et al. [72]). Researchers have found that employees often are not aware that they are violating IT standards or the potential consequences (Beimborn and Palitza [8]; Haag et al. [41]; Haag and Eckhardt [39]) for example concerning violating regulations (Gozman and Willcocks [34]).

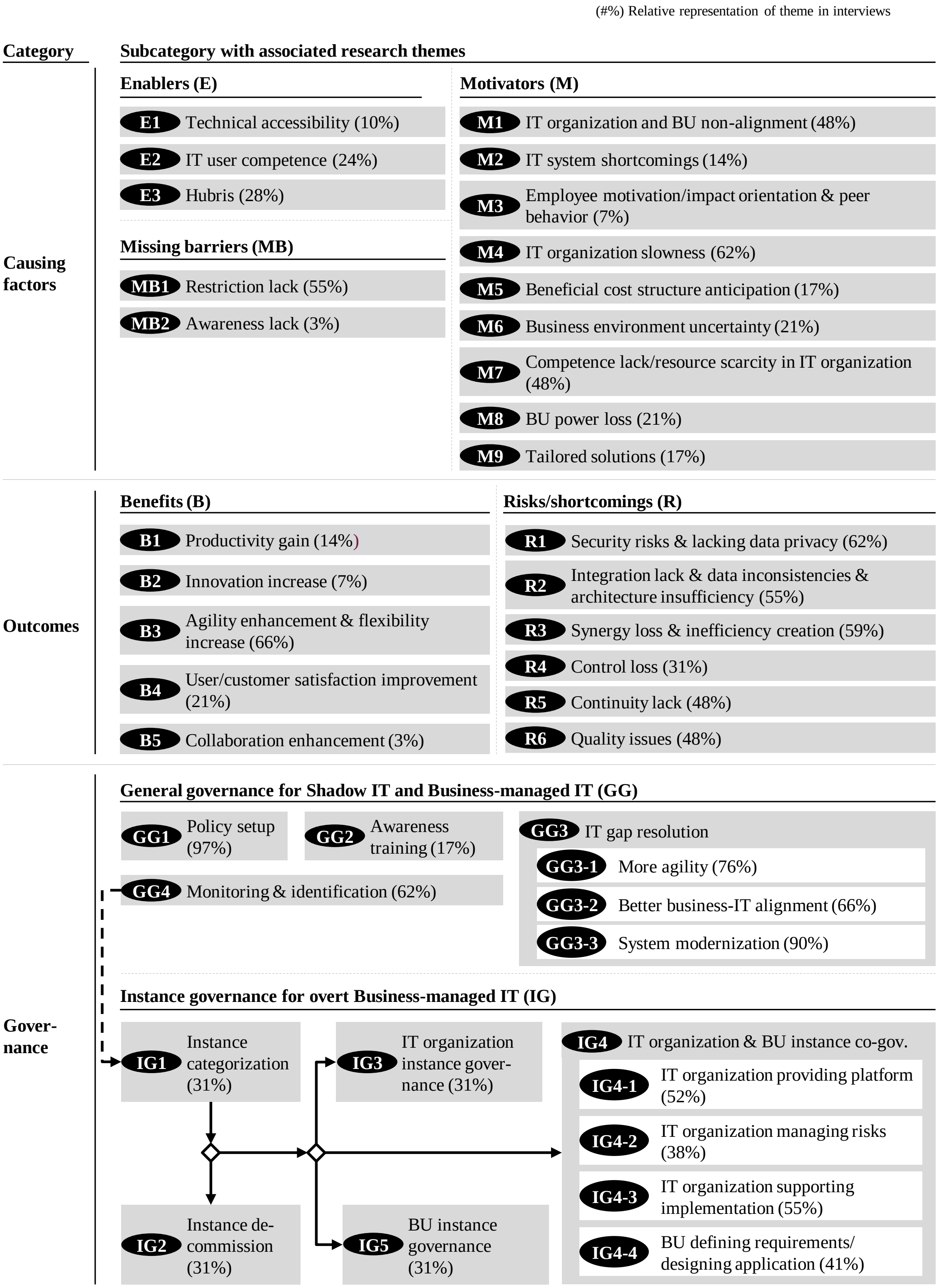

(#%) Relative representation of theme in interviews
Category
Subcategory with associated research themes
Causing factors
Enablers (E)
E1 Technical accessibility (10%)
E2 IT user competence (24%)
E3 Hubris (28%)
Missing barriers (MB)
MB1 Restriction lack (55%)
MB2 Awareness lack (3%)
Motivators (M)
M1 IT organization and BU non-alignment (48%)
M2 IT system shortcomings (14%)
M3 Employee motivation/impact orientation & peer behavior (7%)
M4 IT organization slowness (62%)
M5 Beneficial cost structure anticipation (17%)
M6 Business environment uncertainty (21%)
M7 Competence lack/resource scarcity in IT organization (48%)
M8 BU power loss (21%)
M9 Tailored solutions (17%)
Outcomes
Benefits (B)
B1 Productivity gain (14%)
B2 Innovation increase (7%)
B3 Agility enhancement & flexibility increase (66%)
B4 User/customer satisfaction improvement (21%)
B5 Collaboration enhancement (3%)
Risks/shortcomings (R)
R1 Security risks & lacking data privacy (62%)
R2 Integration lack & data inconsistencies & architecture insufficiency (55%)
R3 Synergy loss & inefficiency creation (59%)
R4 Control loss (31%)
R5 Continuity lack (48%)
R6 Quality issues (48%)
Gover-nance
General governance for Shadow IT and Business-managed IT (GG)
GG1 Policy setup (97%)
GG2 Awareness training (17%)
GG3 IT gap resolution
GG3-1 More agility (76%)
GG3-2 Better business-IT alignment (66%)
GG3-3 System modernization (90%)
GG4 Monitoring & identification (62%)
Instance governance for overt Business-managed IT (IG)
IG1 Instance categorization (31%)
IG2 Instance de-commission (31%)
IG3 IT organization instance gover-nance (31%)
IG5 BU instance governance (31%)
IG4 IT organization & BU instance co-gov.
IG4-1 IT organization providing platform (52%)
IG4-2 IT organization managing risks (38%)
IG4-3 IT organization supporting implementation (55%)
IG4-4 BU defining requirements/ designing application (41%)

Figure 3: Comparison of Research Themes in Literature and Practitioner Perceptions, Literature Perceptions, based on Klotz et al. [51], p. 24

Outcomes

To illustrate the positive and negative outcomes of Shadow IT and Business-managed IT, we differentiate the two subcategories *benefits (B)* and *risks/shortcomings (R)*.

Benefits (B)

B1 Productivity gain. The literature recognizes increased productivity and efficiency as benefits of Shadow IT or Business-managed IT (Ortbach et al. [76]; Röder et al. [86]; Silic [89]; Zimmermann et al. [113]). However, only four participants (P12, P16, P25, P26) (14%) mentioned those benefits. This could be because literature looks at the individual performance (Györy et al. [35]; Mallmann et al. [66]; Ortbach et al. [75]) and the executive IT managers, whom we interviewed, may instead take a high-level organizational perspective. Nevertheless, some recognized the benefit of increased productivity and efficiency through automation of processes with (self-developed) systems and tools that are managed by the users themselves (P12, P16, P25, P26) (Alter [2]). P12, for example, explained that "what can work in an automated way, works. First of all, it takes less time, the resource time is relieved, and on the other hand, the probability of error is much lower". Similarly, P16 mentioned, "people who are programming little things […] to improve local processes and make their lives easier".

B2 Innovation increase. Only two participants (P03, P28) (7%) used the word "innovation" in association with Shadow IT and Business-managed IT, which is often recognized in the literature as a benefit, for example, in Buchwald et al. [16], Fürstenau and Rothe [28], or Thatte et al. [99]. This may be due to the abstract and broad meaning of innovation in different fields. P03 recognized a system created by a BU as an innovative solution and the associated possibility of working more innovatively. More specifically, P28 reported that some new solutions created by BUs were so good that they were rolled out officially in other markets.

B3 Agility enhancement & flexibility increase. The perceived increase in agility, flexibility, and speed of implementation is the by far most prominent (66%) benefit of Shadow IT and Business-managed IT recognized by the participants. Participants, for example, described cases with highly agile, iterative processes (P05, P07, P11) (Khalil et al. [49]; Kopper et al. [56]; Mallmann et al. [66]). They also highlighted the benefit of being able to create solutions very close to the customers/users, which enables the efficient exchange of requirements and designs and avoids the overhead of formalistic organizational processes (P02, P04, P06, P11, P13, P16, P19, P24, P26, P29) (Silic [89]). P06, for example, explained that "[the BU colleagues], they are certainly closer to their sales colleagues, who […] know better what they need. There […] one can also act more agile. You do not need a complex project approach." This also enables more flexibility to find new solutions (P03, P12, P23, P27) (Behrens [6]; Hetzenecker et al. [42]; Huber et al. [45]) and can result in being able to deliver solutions faster (P01, P15, P16, P18, P19, P23).

B4 User/customer satisfaction improvement. 21% of participants mentioned some form of improved user/customer satisfaction. The BUs may, for example, be happy about being able to manage their solutions and to cover their needs directly (P29) (Singh [94]). This may be because they best understand their requirements (P06) or because users attribute a higher quality to self-developed applications (Lyytinen and Newman [63]; McGill [70]). Users might be satisfied with simple solutions that cover their temporary needs (P01) or with the possibility to cover their needs when the IT organization is not able to so (P02, P04). P23 mentioned an example of Business-managed IT, which allowed to inform better and improve the satisfaction of a trading partner. Similar examples of improved customer satisfaction exist in the literature (Ferneley [26]; Silic et al. [92]; Tambo and Bækgaard [98]).

B5 Collaboration enhancement. Enhancement of collaboration is a smaller theme in literature, and only one participant (P11) (3%) explicitly mentioned it. P11 described that during the creation of solutions in BUs, there is an enhanced communication due to the direct peer-to-peer exchange of requirements (Haag et al. [41]). However, that would also be indirectly the case for the examples described for B3. There was no case in our interviews that dealt with knowledge sharing, increased social presence (Mallmann et al. [67]; Mallmann and Maçada [65]), or improved communication due to Shadow IT or Business-managed IT systems (Ologeanu-Taddei et al. [74]; Silic and Back [90]; Steinhüser et al. [97]; Thatte et al. [99]).

Risks/shortcomings (R)

R1 Security risks & lacking data privacy. Participants generally agreed (62%) that one of the most significant risks to covert Shadow IT is data security (P02, P03, P07, P13, P19, P21, P23) (Fürstenau et al. [32]; Haag and Eckhardt [38]; Mallmann et al. [67]). Security standards, guidelines, and authorization concepts are often neglected when BUs implement systems without involving the IT organization (P01, P02, P06, P25, P28). Those aspects are usually hard or impossible to fix after the implementation is finished (P08, P10, P18, P27). This is especially problematic when compliance rules (P15, P19) (Györy et al. [35]; Walters [103]; Zimmermann and Rentrop [109]) or general regulations (Gozman and Willcocks [34]; Kretzer and Maedche [60]; Walters [103]) about data security and privacy (Ebeling et al. [25]; Ologeanu-Taddei et al. [74]; Panko and Port [78]; Röder et al. [85]) in industries such as healthcare or banking are not considered (P06, P08, P13, P24). P24, for example, pointed out that the General Data Protection Regulation requires the ability to delete all data of a customer, which is difficult if data is spread across multiple systems. Shadow systems may also make security monitoring mechanisms ineffective as they exist outside the scope of official architecture (P04) (Zimmermann et al., 2017).

R2 Integration lack & data inconsistencies & architecture insufficiency. Similar to security risks there is also broad agreement among participants (55%) that integration with other systems is often lacking for systems implemented by BUs (P01, P02, P03, P06, P07, P10, P13) (Azad and King [5]; Ebeling et al. [25]; Kopper [54]). The IT organization is only asked later in the process to fix ongoing issues or to create interfaces (P02, P07, P29). However, this may be difficult when the solution is based on poor architectural principles, is not standardized, or is overall complex (P03, P12, P27) (Fürstenau et al. [31]; Fürstenau et al. [29]; Rentrop et al. [84]). In addition, this leads to data inconsistencies, data duplication, and a lack of traceability which is especially problematic in case of regulatory requirements (P05, P06, P09, P11, P13, P15, P20) (Fürstenau et al. [29]; Hetzenecker et al. [42]; Thatte et al. [99]).

R3 Synergy loss & inefficiency creation. This theme was mentioned by 59% of participants. They reported that Shadow IT and Business-managed IT can lead to increased IT costs, for example, due to poor project execution or external vendors taking advantage of the BU's inexperience (P01, P06, P09, P10, P12, P13, P18) (Huber et al. [44]; Silic et al. [92]; Zimmermann et al. [113]). Additional costs furthermore arise when the IT organization needs to fix failed projects or system shortcomings (P01, P06, P08, P10, P12, P13, P18). Inefficiencies are also caused by system redundancies and overlaps (P19, P22, P27, P28) (Chua et al. [19]; Peppard [79]; Thatte et al. [99]), which prevent synergies (P06) (Györy et al. [35]; Kretzer [59]; Kretzer and Maedche [60]). Similarly, inefficiencies in the procurement process can emerge (P08, P10, P21, P23). Additionally, lower degrees of standardization lead to higher complexity, a heterogeneous IT landscape, inconsistent user- and customer experiences, and higher architectural costs (P01, P03, P23, P24) (Fürstenau et al. [31]; Fürstenau et al. [29]; Huber et al. [45]). A heterogeneous IT landscape also increases the effort required to align interfaces between systems (P29).

R4 Control loss. Loss of control was brought up by 31% of participants. Due to the lack of transparency of Shadow IT (P15) (Gozman and Willcocks [34]; Zimmermann et al. [113]), it gets more challenging to apply governance principles about architecture, compliance, or security (P02, P29) (Khalil et al. [49]; Kopper et al. [56]; Lund-Jensen et al. [62]). Especially small systems remain easily hidden and are hard to control (P12, P26). The participants also reported that it is difficult or almost impossible to gain back control after it is lost (P03, P05, P09). An example of that are dependencies on vendors for future system changes (P01) (Fürstenau et al. [32]; Khalil et al. [49]; Walterbusch et al. [102]). In literature, additional downsides include undermining of management intentions (Röder et al. [85]) or strategic goals (Chua and Storey [18]; Zimmermann and Rentrop [108]) and shifting power relations (Azad and King [4]; Fürstenau et al. [29]; Khalil et al. [49]).

R5 Continuity lack. Almost half of all participants (48%) identified continuity risks, especially for covert Shadow IT. As business processes depend on the availability of IT systems, operational stability is a high risk (P06, P13), specifically with highly integrated systems or in critical areas such as production processes (P03, P07, P28). Systems are also often created by single or few persons, and continued operation depends on them (Behrens, 2009; Fürstenau, Rothe et al., 2016; McGill, 2004). Issues, therefore, arise when those persons leave the company or even unexpectedly pass away (P01, P02, P03, P04, P12, P16, P26) notably if proper documentation is missing (P03, P16) (Fürstenau et al. [29]; Rentrop et al. [84]). Issues through lack of maintainability, support, or missing maintenance contracts with vendors often arise long after the creation of a system, e.g., when errors occur through operating system upgrades or deprecation of underlying frameworks (P02, P03, P06, P07, P18, P26) (Fürstenau et al. [32]; Györy et al. [35]). Issues and conflicts can also emerge when knowledge transfer or additional expertise is required when transferring the operation of a system to the IT organization (P14, P15).

R6 Quality issues. Not identified in literature but emerged in half of the interviews (48%) are quality issues with systems created by BUs. It is a more general factor that includes some aspects of other risks (*R1 Security risks & lacking data privacy*, *R2 Integration lack & data inconsistencies & architecture insufficiency*). However, it primarily refers to poor overall system quality and inadequate coverage of the original requirements. Systems are usually created by people in BUs who are not familiar with professional software development practices. Standard principles such as testing, documentation, code versioning, code review, error handling, or quality assurance in every phase are therefore often neglected (P01, P03, P06, P12, P21, P29). There may be a focus on the frontend, but backend quality can suffer due to inconsistent data models or lack of modularization (P01, P11), which leads to errors in production (P18, P22). Also, typical non-functional requirements such as system performance or data backup may be ignored (P03, P10, P13, P18, P20, P23).

Other outcomes. Some smaller themes for outcomes were identified as well. While not identified by a significant number of participants, Business-managed IT may indeed realize economic benefits and constitute a proportionate solution for local requirements (Silic et al. [92]; Tambo and Bækgaard [98]), for example, by allowing the IT organization to focus on its core responsibilities without having to implement every small requirement in a process-heavy manner (P02, P07, P15, P26). Other adverse outcomes can include issues with branding standardization towards the customer (P20, P23), traceability of transactions in the case or regulatory requirements (P13), or licensing issues (P23). Other outcomes described in the literature include political conflicts in companies (Behrens [6]; Houghton and Kerr [43]; Jones et al. [47]) or severe changes in the IT landscape due to a heterogeneous architecture (Fürstenau et al. [32]; Singh [94]).

Governance

We distinguish two governance subcategories for Shadow IT and Business-managed IT: First, general governance measures for Shadow IT and Business-managed IT (GG) exist, regardless if instances are overt or covert. Second, if instances are overt, for example, after being identified, more specific governance measures can be applied (Fürstenau et al. [30]), that is, *instance governance measures for overt Business-managed IT (IG).* Overt instances can be categorized (IG1), and two potential governance decision points exist: Instances can be decommissioned (IG2) or continued. If instances are continued, the governance responsibility can be allocated to the IT organization (IG3), assigned in a co-governance model between the IT organization and the BU (IG4), or it can be allocated to the BU (IG5). A co-governance model (IG4) can also be chosen to generally allow and enable the creation of (future) Business-managed IT.

General Governance for Shadow IT and Business-managed IT (GG)

GG1 Policy setup. Virtually all participants (97%) talked about policies in some form to govern Shadow IT and Business-managed IT. Participants recognized that it is essential to delimit IT task responsibilities between BUs and the IT organization by using a corresponding policy. Some have clearly defined rules (P04, P08, P15, P16, P22, P26, P29), but others find it challenging to formalize a clear delimitation (P02, P03, P09, P19, P21). P02, for example, said, “if you could define these boundaries so clearly and if they are respected, I think there would be no Shadow IT.” Consistent with the definition for Business-managed IT, some participants classify systems created by BUs outside of the defined governance rules as Shadow IT (P16, P19, P24). Especially the managing board (P21, P23) requires a collective agreement of the policy. A policy’s effectiveness is also increased when IT budget rules are enforced (P10, P24, P26). To enforce the rules on an individual level, it is also possible to let employees sign the policy and to take disciplinary action in case of infringement or at least issue a warning (P12, P21). However, some are not in favor of a strict governance policy as it would negatively affect organizational flexibility (P01, P15). For Business-managed IT, the participants broadly agree that there needs to be some form of central control (Fürstenau et al. [32]; Györy et al. [35]). Common types include architecture boards, project portfolio boards, or governance boards where IT and business representatives together review and decide on IT initiatives. The IT organization can, for example, veto on IT architecture issues. In its most basic form, at least requirements and initiatives are coordinated from a central perspective to avoid duplicated systems, enable synergies, and increase standardization (P01, P05, P07, P08, P10, P11, P13, P16, P19, P21, P23, P27). As a prerequisite, approval guidelines for Business-managed IT are commonly defined. Those may include security, architecture, testing, or contracting standards the BUs need to adhere to (P02, P04, P05, P06, P08, P16, P17, P20, P24, P28). Outside of projects, policies can also define which tools, devices, or services are allowed or prohibited for usage in the organization (P04, P12, P24, P25). However, literature generally supports the notion that a prohibition of Shadow IT and Business-managed IT does not seem reasonable in most cases (Zimmermann et al. [111]; Zimmermann et al. [113]), as this would negatively impact the motivation of employees (Haag et al. [41]) and innovation behavior (Köffer et al. [52]).

GG2 Awareness training. The relatively low popularity of this factor (only mentioned by 17% of the participants) is consistent with the findings for GG1. To be able to create awareness of policies (Haag et al. [41]; Kopper [54]; Silic et al. [92]) and to minimize potential threats of unapproved IT, they need to be clearly defined in the first place. However, as previously described, that is often not the case. If policies are sufficiently defined, one possibility is to continuously educate users about them through personal communication (P01, P17) or to directly confront them in case of policy violations (P12). Alternatively, they can be communicated through training courses as part of the onboarding process or through annual, mandatory IT (security) training (P21, P24) (Gozman and Willcocks [34]; Rentrop et al. [84]; Silic and Back [90]).

GG3 IT gap resolution. In literature, there is only a small focus on reducing the need for Shadow IT (or Business-managed IT) by addressing existing IT system shortcomings and better fulfilling unmet needs (Walterbusch et al. [101]; Walterbusch et al. [102]; Zimmermann and Rentrop [108]). However, the participants discussed this topic more prominently and nuanced during our interviews. Due to that, we split the findings into three parts (*GG3-1 More agility*, *GG3-2 Better business-IT alignment*, and *GG3-3 System modernization*) and describe them in the following.

GG3-1 More agility. One of the primary motivators for Shadow IT is *M4 IT organization slowness*. The participants (76%), therefore, aim to or are already improving their IT organizations' agility, for example, by working with agile development methods. To better fulfill their users' needs they (plan to) employ shorter iteration cycles and use integrated teams which consist of both IT and business employees that are closely working together (P01, P02, P11, P13, P14, P17, P18, P20, P21, P22, P24, P26). Teams can, for example, be organized around product owners (P25, P27). Some participants described a bimodal approach where specific systems still require a more stable, linear process (P07, P22). Others highlighted the need to act flexible to requirements, to work closely with the BUs, and to create business value, which is more critical than lowering IT costs (P03, P05, P15). Two participants preferred to keep development in-house and avoid outsourcing to be able to act faster and closer to the business (P23, P29). P29 explained in this context: "Only [having the competence in-house] puts me in a position to respond to the requests of the business areas at the required speed." P10 also noted that they are shifting their focus to application development away from infrastructure management. Even before development, faster initial prioritization, and communication of decisions prevent users from seeking other ways to fulfill their needs. This includes telling the users promptly if a request must be denied, a potential timeline, or if a solution can be implemented locally or requires global coordination (P14, P15, P16). It can similarly help to act fast and proactively anticipate the users' needs (P20): "[…] want to be ahead of the game before a [user] begins to feel the need to look around the market for solutions".

GG3-2 Better Business-IT alignment. In addition to agility, 66% of the participants highlighted the need for good business-IT alignment, which similarly addresses one of the primary motivators of Shadow IT (see *M1 IT organization and BU non-alignment*). The arguments made by the participants mostly resemble the factors for business-IT alignment maturity, as defined by Luftman [61]. Better communication between the IT organization and BUs helps to exchange ideas and to create transparency (P05, P09, P14, P16, P26) (Walterbusch et al. [101]; Walterbusch et al. [102]). Some also highlighted the importance of understanding their users' business processes to be able to speak a "common language" (P05, P10, P16, P28) (Zimmermann and Rentrop [108]). Ideally, the IT organization is considered a partner (P05, P07, P10, P13, P23, P28) and working closely together with the BUs (P05, P11, P15, P27, P28) instead of being perceived as a mere cost factor. The IT organization, therefore, needs to demonstrate its business value (P05) and build a trust-based relationship that prevents an environment where BUs need to hide Shadow IT (P01, P16, P25). However, that can be a challenge based on the organizational culture of individual units (P04). A mature governance process, which involves both the IT organization and the BUs, also helps to retain transparency and to quickly prioritize requests (P03, P07, P10, P12, P16).

GG3-3 System modernization. 90% of the participants brought this theme up in some form. Many, for example, highlighted "cloud" as a factor in modernizing their IT architecture (P01, P04, P11, P17, P18, P19, P22, P24, P25, P26, P27, P29). This does not necessarily mean public cloud, but generally cloud-based delivery models (including private cloud) that allow more agility (Walterbusch et al. [102]). The same goal should also be achieved by a stronger modularization of systems, for example through loosely coupled microservices (P01, P13, P15, P19, P22), or integration services that allow more flexibility (P06, P11). The participants also focus on improving or replacing systems to cover better users' current requirements (P13, P16, P23, P25). P20, for example, saw a significant drop in the need for Shadow IT after providing different solutions that filled existing functionality gaps. P26 expressed the approach to systematically evaluate gaps in official systems by analyzing the functionality in existing spreadsheet-based macros. Some participants highlighted that proactively evaluating and providing new solutions (for example, collaboration tools) prevents users from procuring their solutions (P09, P21, P24). P25, for example, operates a community platform to collect feedback and ideas for new systems, and P27 actively maintains a whitelist on tools that employees can use. However, some also deal with (or dealt with) "old" problems such as standardizing inhomogeneous legacy systems and organizational IT processes to increase efficiency (P02, P04, P05, P06, P08, P10, P13, P14).

GG4 Monitoring & identification. 62% of the participants described some form of technical measures that can be used to enforce policies on Shadow IT (Röder et al. [86]; Silic and Back [90]; Walters [103]). While so-called "cloud access security brokers" are popularly dealt with in practitioner literature as a tool for network monitoring and access control to cloud services (Kopper et al. [58]), none of the participants mentioned using one. While some of them described network monitoring to identify unsanctioned cloud services and security threats (P23, P25, P29), others actively block certain services from file storage or infrastructure providers (P12, P13, P14, P21, P22) (Kopper [54]). However, for some, the identification of Shadow IT is just a side effect of general security measures such as keeping track of software versions and updates or data access control (P03, P04, P10, P16, P20, P24). On the individual device level, endpoint monitoring and policy enforcement through device management tools is a standard method (P12, P14, P24, P27) (Silic and Back [90]), for example, to also keep software licensing under control (P04). P07 described a high level of visibility of Shadow IT because BUs cannot easily access any external infrastructure services and would have to request server capacity officially. Visibility is also given when BUs ask for help with integrating their solutions with other systems, for example, through help desk requests (P07, P26) (Rentrop and Zimmermann [82]). In general, monitoring can be seen as a measure to identify covert Shadow IT instances, and henceforth, the instances become overt, and thus, Business-managed IT (Kopper et al. [55]; Kopper et al. [56]).

Instance Governance for Overt Business-managed IT (IG)

IG1 Instance categorization. Identified Shadow IT or overt Business-managed IT can be categorized along different criteria to determine how to govern them (for examples see Buchwald and Urbach [13]; Buchwald and Urbach [14]; Lund-Jensen et al. [62]; Mallmann et al. [66]; Mallmann et al. [67]; Rentrop et al. [84]; Röder et al. [86]). This was discussed by 31% of the participants. In our interviews, some of them had clearly defined processes to evaluate identified Shadow IT (P10, 28). This can include general risk assessments that take into account the criticality (P13) (Ferneley and Sobreperez [27]; Melo et al. [71]; Rentrop and Zimmermann [83]), aspects around security (P25), or the scope of the instance (Fürstenau et al. [30]). Another factor might be costs (P10, P26) or the number of resources required to operate the system (non-standard systems require additional expertise) (P14). P08 explained that identified systems are not shut down immediately, but collaboratively assessed with the users how to legitimize them. P11 highlighted that it was essential to involve the executive board in the strategic decision about the future use of a large shadow system.

IG2 Instance decommission. In some cases, the assessment of a Shadow IT instance can result in a decision for its decommission, for example, because the risks or shortcomings are deemed too high for continued operation (Fürstenau et al. [32]; Fürstenau et al. [29]; Kopper [54]). However, in all interviews that described decommissions (31%), instances were replaced by other systems so that no functionality gap was left behind. After all, those systems exist because they cover unmet needs. Examples include replacing inadequate systems with standard products (P12, P14), providing alternative solutions for failed system implementations (P18), or consolidation of historically grown, dispersed systems (P10, P16). Some participants focus on a highly collaborative approach to finding an alternative, secure solutions together with the BUs because they recognize the users' unfulfilled needs and that the previously provided systems were not adequate (P25, P26). P28 and P29 explained that decommissioning and replacing the systems in question is more challenging from a communication and acceptance perspective than from a technical perspective.

IG3 IT organization instance governance. If an instance is decided to be continued, one of three possible governance solutions is the transfer of the instance governance to the IT organization (Behrens [6]; Zimmermann et al. [110]; Zimmermann et al. [113]), including a migration to the official infrastructure (P08, P09, P10, P23). This was described by 31% of the participants. In some cases, the BU requested the IT organization to take over the operation (Singh [94]) only after the system development was finished. However, participants had doubts about supporting inadequate solutions continuously (P03, P05). In other cases, the IT organization was required to step in during failed implementation projects, for example, because integration with other systems was missing, requirements inadequately covered, costs overrun (P01, P13), or crucial security concerns existed (Chua et al. [19]). P02 described a case where a system needed to be taken over because compatibility issues arose due to system updates, and P13 integrated a vendor in their organization who was previously working on Shadow IT directly with the BUs.

IG4 IT organization & BU instance co-governance. Besides IG3 IT organization instance governance, another possibility is co-governance between the IT organization and the BUs. This describes allocating the responsibility of individual service components or tasks of Business-managed IT to either the IT organization or the BUs (Zimmermann et al. [112]). We detail specific tasks and their typical allocation in the following themes.

IG4-1 IT organization providing platform. To ensure standardization and allow economies of scale, 52% of the participants describe providing common platforms for IT projects of BUs in different levels of abstractions, for example in the form of infrastructure that is centrally secured and supported (P04, P05, P15, P16, P19, P21, P23, P25, P27, P29) (Bygstad [17]; Chua and Storey [18]; Kopper et al. [56]). P04 explained this as a similar mechanism that is already well established with public cloud providers, which can ensure specific standards and security levels to their customers. Some participants provide services including the database layer in the technology stack to achieve synergies (P04, P17, P29) (Kopper [54]; Zimmermann et al. [111]; Zimmermann et al. [112]). P06 provides an integration service for BUs where the IT organization is managing the complex data integration layer with core systems and provides the necessary processes and tools (Chua and Storey [18]). P23 offers common frameworks that can be adapted by local e-commerce teams. Others similarly provide platforms that can be customized for local requirements (e.g., voting platform) or standardized .NET development environments for BU projects (P02, P06, P17). With self-service BI platforms, users can build their reports and conduct analyses (P16, P26). P07 and P11 mentioned potential future use of so-called “low-code” platforms that provide a standardized environment where security, privacy, and integration aspects can be centrally managed. Advanced users would be able to implement applications themselves (without needing expert programming knowledge) and to leverage the speed, agility, and flexibility advantages. The closest example of such a setup in the interviews was a cloud-based CRM platform where users can build their reports, dashboards, and workflows without heavy coding (P11). P25 even suggested that getting infrastructure from cloud providers may be a procurement topic (with oversight of the Chief Information Security Officer and policies) in the future, which would leave out the CIO or the IT organization in the process. Also, a framework for the governance of “spreadsheet-based end-user applications” could be considered a platform for governing Business-managed IT (Raković [80]).

IG4-2 IT organization managing risks. In a co-governance model with the BUs, the IT organization would still be responsible for aspects around security, data protection, and licensing (mentioned by 38% of the participants) (Kopper et al. [56]; Silic et al. [92]). Those are areas that should uniformly be ensured centrally (P04, P06, P07, P25). This is, for example, required for infrastructure which needs to be vetted by external certification bodies (P17). Global security standards (in addition to architectural standards) for BU projects are also commonly defined (P06, P07, P16, P21, P27). Some participants foresee a dedicated function or role that makes sure that those (data security and privacy) standards are adhered to, that coordinates security aspects across units, and that provides expertise (P02, P23, P29).

IG4-3 IT organization supporting implementation. Described by 55% of the participants, the IT organization may provide support for BU IT projects, for example, in the form of expertise about professional software development, architectural design, or security (P02, P04, P07, P11, P12, P17, P21, P23, P29) (Chua and Storey [18]; Panko and Port [78]; Zimmermann et al. [113]). This makes especially sense for complex topics, which require deep technical expertise or heavy coding (P11, P21). One example is integration with other systems, which should remain the responsibility of the IT organization (P06, P07, P11, P23, P29). Vendor management and procurement are also areas that are best managed centrally to achieve synergies and economies of scale (P06, P13, P16, P23, P27, P29). Independent of the actual degree of involvement, some participants argued that they should be involved in any case (P02, P21, P26), at least for the initial conceptualization (P13) or for the architectural design and the overall portfolio management (P27). Other possibilities for involvement include support for testing (P06), project management (P15), and centrally providing helpdesk support for Business-managed IT (P28).

IG4-4 BU defining requirements/designing application. This theme complements the tasks described in the previous three areas of co-governance (and was mentioned by 41% of the participants in some form). BUs can, for example, be responsible for developing their own (local) applications (Andriole [3]; Chua et al. [19]; Silic et al. [92]), which are hosted on or take advantage of a platform (e.g., infrastructure, database, integration service) provided by the IT organization (P04, P06, P16, P17, P19). Similarly, BUs can take over customizing e-commerce frameworks, CRM, ERP, or SharePoint systems that are provided by the IT organization, which also takes care of integration with other systems (P06, P11, P17, P23, P25). Another form is the creation and customization of reports that build on top of databases (P05, P07). There are different degrees of responsibility split. In some cases, BUs can be mostly responsible for building applications specific to their requirements, and the IT organization is only involved where necessary (P21). If a BU is working directly with an external vendor, the IT organization would still take over governance, integration, and architectural validation (P07). In other cases, the IT organization is more actively involved, for example, in integrated teams that are organized around product owners that belong to BUs (P25), or in joint R&D projects (P15). The BUs can also at least be responsible for requirements engineering (P21) (Kopper et al. [56]; Zimmermann et al. [111]; Zimmermann et al. [112]).

IG5 BU instance governance. In some cases (described by 31% of the participants), BUs can be largely autonomous in managing IT systems with specific guidelines to adhere to and interfaces to use (Andriole [3]; Györy et al. [35]; Zimmermann et al. [110]), for example, when the organization is generally decentralized or when experimenting with new ventures (P04, P23, P25, P28). However, that is also associated with responsibilities for any adverse consequences (P29). BUs (or separate units) are also commonly entirely responsible for "product IT" (or generally R&D, including IT as products or IT for tangible products for customers) or "shop floor IT" (management of CNC machines, systems at the production lines, and grapplers) (P02, P04, P24). Furthermore, the BUs may manage systems that are highly specific to their requirements (Winkler and Brown [105]; Zimmermann et al. [113]). They usually have sufficient IT skills and benefit from their deep business expertise to be able to locally develop and support the systems (P04, P08, P09, P27, P29). It may also be decided that a system can remain in the control of a BU because the use case is only non-critical and small (P28). While the degree of responsibility for the BUs is high for the examples just discussed, they can still request support from the IT organization for complex issues as described in *IG4-3 IT organization supporting implementation*.

DISCUSSION

In this section, we discuss the differences in major themes between literature and interviews; that is, the difference in the frequency they were observed in the two areas. To compare the relative importance of themes in both areas, we contrast the major themes, i.e., themes which are part of the top third of (relative) frequency in literature or respectively in the interviews. For each theme, Figure 4 indicates the number of (and relative frequency of) occurrences, in both literature and the interviews. Figure 4 (and Figure 3), therefore, identify themes that are in the top third for the interviews but not in the literature (▲) and vice-versa (▼). It also indicates if themes are consistently classified as major themes (●) or not as major themes (—) in both literature and the interviews. Additional themes identified in the interviews are highlighted as well (✦). Consequently, Figure 4 highlights and compares the major themes in the literature and of the interview participants and all additional themes that emerged during the interviews.

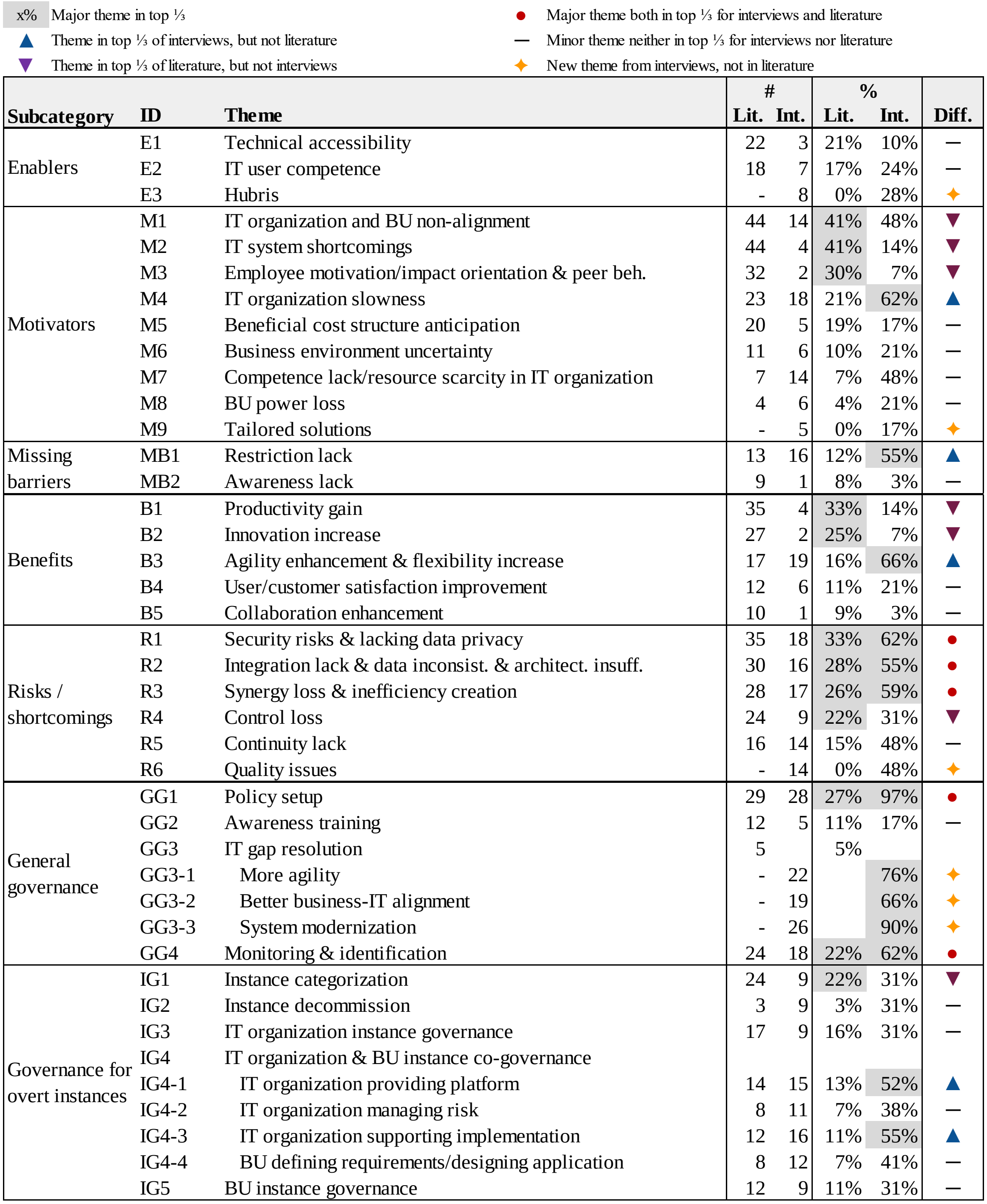
Causing factors

E3 Hybris (✦) is an additional enabler identified in the interviews, which did not occur in literature at all. *E2 IT user competence* (—) implies that actual ability contributes to the emergence of Shadow IT and Business-managed IT. However, hubris indicates that BUs overestimate their IT competencies and engage in their own IT projects because they are convinced to do a better job than the IT organization. In the end, both factors have been mentioned with similar frequency in the interviews.

The primary motivator for Shadow IT and Business-managed IT identified in the interviews is *M4 IT organization slowness* (▲), which was not a major theme in literature. In contrast, three further major themes in literature are not part of the top third themes in the interviews: *M1 IT organization and BU non-alignment* (▼), *M2 IT system shortcomings* (▼), and *M3 Employee motivation/impact orientation & peer behavior* (▼). For example, M2 is less frequent as the practical examples deal with new systems (covering novel use cases) rather than with shortcomings about existing systems.

An additional motivator identified in the interviews is *M9 Tailored solutions* (✦). It is only mentioned by 17% of participants, but still gives additional insights for potential motivators. It indicates that in some cases, BUs do not want to make any compromises for the sake of standardization (or other tradeoffs resulting from constraints dictated by the IT organization) and look for solutions that exactly match their needs.

In terms of missing barriers, *MB1 Restriction lack* (▲) was a significant factor in the interviews in contrast to literature. The main issue is, therefore, a missing clarity in policies about Shadow IT and Business-managed IT. *MB2 Awareness lack* (—) is less of a problem because, for that, the policies need to exist in the first place.



x% Major theme in top ⅓

▲ Theme in top ⅓ of interviews, but not literature

▼ Theme in top ⅓ of literature, but not interviews

● Major theme both in top ⅓ for interviews and literature

— Minor theme neither in top ⅓ for interviews nor literature

✦ New theme from interviews, not in literature

			#		%		
Subcategory	**ID**	**Theme**	**Lit.**	**Int.**	**Lit.**	**Int.**	**Diff.**
Enablers	E1	Technical accessibility	22	3	21%	10%	—
	E2	IT user competence	18	7	17%	24%	—
	E3	Hubris	-	8	0%	28%	✦
Motivators	M1	IT organization and BU non-alignment	44	14	**41%**	48%	▼
	M2	IT system shortcomings	44	4	**41%**	14%	▼
	M3	Employee motivation/impact orientation & peer beh.	32	2	**30%**	7%	▼
	M4	IT organization slowness	23	18	21%	**62%**	▲
	M5	Beneficial cost structure anticipation	20	5	19%	17%	—
	M6	Business environment uncertainty	11	6	10%	21%	—
	M7	Competence lack/resource scarcity in IT organization	7	14	7%	48%	—
	M8	BU power loss	4	6	4%	21%	—
	M9	Tailored solutions	-	5	0%	17%	✦
Missing barriers	MB1	Restriction lack	13	16	12%	**55%**	▲
	MB2	Awareness lack	9	1	8%	3%	—
Benefits	B1	Productivity gain	35	4	**33%**	14%	▼
	B2	Innovation increase	27	2	**25%**	7%	▼
	B3	Agility enhancement & flexibility increase	17	19	16%	**66%**	▲
	B4	User/customer satisfaction improvement	12	6	11%	21%	—
	B5	Collaboration enhancement	10	1	9%	3%	—
Risks / shortcomings	R1	Security risks & lacking data privacy	35	18	**33%**	**62%**	●
	R2	Integration lack & data inconsist. & architect. insuff.	30	16	**28%**	**55%**	●
	R3	Synergy loss & inefficiency creation	28	17	**26%**	**59%**	●
	R4	Control loss	24	9	**22%**	31%	▼
	R5	Continuity lack	16	14	15%	48%	—
	R6	Quality issues	-	14	0%	48%	✦
General governance	GG1	Policy setup	29	28	**27%**	**97%**	●
	GG2	Awareness training	12	5	11%	17%	—
	GG3	IT gap resolution	5		5%		
	GG3-1	More agility	-	22		**76%**	✦
	GG3-2	Better business-IT alignment	-	19		**66%**	✦
	GG3-3	System modernization	-	26		**90%**	✦
	GG4	Monitoring & identification	24	18	**22%**	**62%**	●
Governance for overt instances	IG1	Instance categorization	24	9	**22%**	31%	▼
	IG2	Instance decommission	3	9	3%	31%	—
	IG3	IT organization instance governance	17	9	16%	31%	—
	IG4	IT organization & BU instance co-governance					
	IG4-1	IT organization providing platform	14	15	13%	**52%**	▲
	IG4-2	IT organization managing risk	8	11	7%	38%	—
	IG4-3	IT organization supporting implementation	12	16	11%	**55%**	▲
	IG4-4	BU defining requirements/designing application	8	12	7%	41%	—
	IG5	BU instance governance	12	9	11%	31%	—

Figure 4: Comparison of Research Themes in Literature and Practitioner Perceptions, Research Themes in Literature, based on Klotz et al. [51], p. 40

Outcomes

Consistent with the finding that *M4 IT organization slowness* (▲) is the primary motivator for Shadow IT and Business-managed IT, *B3 Agility enhancement & flexibility increase* (▲) is indeed seen as the main benefit. While *GG3-1 More agility* (✦) describes addressing the underlying motivator by improving the agility, speed, and flexibility of the IT organization, participants still recognize Shadow IT and Business-managed IT as achieving a similar goal. In contrast, *B1 Productivity gain* (▼) and *B2 Innovation increase* (▼) were less prominent benefits, which may be due to the very individual perspective about productivity in the literature (in contrast to the high-level view of our executive participants) and due to the abstract meaning of innovation.

The main three risks identified in literature also consistently emerged as the main three risks identified in the interviews*: R1 Security risks & lacking data privacy* (●), *R2 Integration lack & data inconsistencies & architecture insufficiencies* (●), and *R3 Synergy loss & inefficiency creation* (●). Only *R4 Control loss* (▼) was not a major theme in the interviews in contrast to literature. This might be because control is a somewhat abstract theme, and other risks such as the initially mentioned ones contribute to it.

R6 Quality issues (✦) emerged as an additional theme that was mentioned by half of the participants but is not apparent in the literature. It partially resembles other risks such as security and integration issues but stands for overall poor system quality and not covering the requirements the system was initially intended. This is because Shadow IT and Business-managed IT is often created by people who are not familiar with professional software development practices.

Governance

Consistent with the missing barrier *MB1 Restriction lack* (▲), the general governance measure *GG1 Policy setup* (●) emerged as a major theme in the interviews, which was mentioned by almost all participants. This highlights the need to set up clear policies (including restrictions), responsibilities, and guidelines. Such measures would also make it easier to differentiate between (covert) Shadow IT and (overt) Business-managed IT and would allow defining appropriate governance mechanisms.

In contrast to the literature, participants also put a strong focus on addressing the motivators for Shadow IT and Business-managed IT by improving their own IT organization. The theme *GG3 IT gap resolution*, which occurred in only 5% of literature items, was therefore split into three parts due to their prominence: *GG3-1 More agility* (✦), *GG3-2 Better business-IT alignment* (✦), and *GG3-3 System modernization* (✦). They can respectively be viewed as addressing the motivators *M4 IT organization slowness*, *M1 IT organization and BU non-alignment*, and *M2 IT system shortcomings*.

GG4 Monitoring & identification (●) resulted in a major theme in both literature and interviews. It primarily describes technical measures to gain transparency on the systems used in the organization (making them overt) and to be able to enforce existing policies.

In terms of governance for overt instances, criteria for *IG1 Instance categorization* (▼) were less prominently mentioned in the interviews. This could be due to the general lack of clearly defined policies (see *MB1*). However, two themes significantly more common in the interviews were *IG4-1 IT organization providing platform* (▲) and *IG4-3 IT organization supporting implementation* (▲). This is most likely the case because the interviews explicitly dealt with both overt and covert forms of IT managed by BUs, and most academic research has focused on (covert) Shadow IT so far.

Category-spanning themes

In summary, the interview participants mentioned three category-spanning (Klotz [50]) themes across causing factors, outcomes, and governance: (a) Business-IT alignment (i.e., *M1*, *GG3-2*), (b) agility (i.e., *M4*, *B3*, *GG3-1*), and (c) policies (i.e., *MB1*, *GG1*). (a) Poor business-IT alignment (*M1*) is a prominent motivator for Shadow IT and Business-managed IT in literature and interviews (although just barely a major theme in the interviews). Hence, the improvement of business-IT alignment is perceived as one of the major themes for general Shadow IT and Business-managed IT governance (*GG3-2*). (b) Furthermore, lacking agility of the IT organization (*M4*) motivates BUs to deploy/procure IT systems autonomously. Agility increase is indeed perceived as a major benefit of Shadow IT and Business-managed IT (*B3*). However, one of the major governance measures is also to increase the agility of the IT organization (*GG3-1*) to address the respective motivator. (c) Besides, missing restrictions or generally a lack of clear policies (*MB1*) as well as a lack of awareness for these (*MB2*) make it challenging to control Shadow IT and Business-managed IT. Thus, the participants identify policies (*GG1*) as the most important theme for the general governance of Shadow IT and Business-managed IT.

CONCLUSION AND OUTLOOK

In this paper, we extend the existing framework of causing factors, outcomes, and governance for Shadow IT and Business-managed IT (Klotz et al. [51]; Kopper and Westner [57]) with practitioner perceptions. In principle, we can confirm the existing framework with the three categories causes, outcomes, and governance with their research themes. The subcategories of causing factors are also perceived by IT managers to be enablers, motivators, and missing barriers. Concerning outcomes, benefits, and risks/shortcomings are the major themes, for which practitioners put more emphasis on risks/shortcomings (see Figure 4). Subcategories of governance are general governance for Shadow IT and Business-managed IT as well as for instance governance for overt Business-managed IT.

The paper contributes to the existing body of research on Shadow IT and Business-managed IT by validating and extending the themes in academic research. In terms of causing factors, we extend the current research themes with *E3 Hubris*, which describes hubris of the BUs as an additional enabler, and *M9 Tailored solutions*, which represent the unwillingness to make functional trade-offs for the sake of standardization, as a further motivator. Concerning outcomes, we additionally identified *R6 Quality issues* as a risk/shortcoming, which refers to overall poor system quality and a lack of covering the original requirements. In terms of governance themes, we found – in contrast to literature – that practitioners put a strong focus on improving their own IT organization to address the motivators for Shadow IT and Business-managed IT. We, therefore, introduce more granular themes for *GG3 IT gap resolution*, that is, *GG3-1 More agility, GG3-2 Better business-IT alignment, and GG3-3 Systems modernization.*

The contributions for practitioners are twofold: First, the framework provides practitioners with a more nuanced understanding of the two phenomena Shadow IT and Business-managed IT as we detail the origins with causing factors, the results as outcomes, and show existing governance approaches. Second, we provide two specific recommendations for practitioners based on the insights from our interviews: (a) Practitioners can address the motivators for Shadow IT by improving the IT organization. If a company increases agility, improves business-IT alignment, and deploys better systems, the motivation for Shadow IT decreases to fill existing gaps (Behrens and Sedera [7]). (b) Furthermore, practitioners can make use of the added agility associated with Business-managed IT. The findings from our interviews suggest that clear policies need to be set up, and co-governance models have to be implemented for the effective use of Business-managed IT (Klotz et al. [51]). At the same time, these measures can mitigate the risks of Shadow IT.

Some limitations need to be kept in mind for the results of our study. We primarily interviewed CIOs and IT managers who tend to be more critical of co-governance models than other stakeholders such as business managers or end-users (Andriole [3]; Khalil et al. [49]). As our interviews were conducted with IT managers, mostly from German-speaking countries, that is, the DACH area (Germany, Austria, Switzerland), the perceptions could be different globally due to regional and cultural differences. Moreover, a comparison of occurrences of the key themes across academic literature and practitioner interviews is difficult. Existing research might focus on selected factors, and the interviews consistently dealt with the whole spectrum of factors (but leaning towards governance aspects).

Moreover, the focus of academic research themes is not perfectly aligned with practitioner perceptions. For example, innovation as an abstract benefit of Shadow IT and Business-managed IT is prominent in academia, but practitioners mention more specific benefits such as agility increase. Increased agility is also a motivator for the study participants to support Business-managed IT and to employ co-governance approaches. Those are addressed by half of the participants, but they are not yet prominently reflected in literature. However, researchers, for example, increasingly deal with the question of splitting IT task responsibilities between the IT organization and the BUs (Zimmermann et al. [111]). Therefore, we propose four avenues for future research based on our findings.

First, the additional themes identified through the practitioner interviews, which are currently not covered in existing literature, could potentially be covered by future research: *E3 Hubris* of users/business managers as an enabler for Shadow IT, *M9 Tailored solutions* motivating Shadow IT and Business-managed IT, *R6 Quality issues* of Shadow IT or Business-managed IT instances, and a more detailed study of *GG3 IT gap resolution* with the three angles *GG3-1 More agility, GG3-2 Better business-IT alignment,* and *GG3-3 System modernization.*

Second, future studies can investigate the three category-spanning themes, which we identified in our practitioner interviews, to provide an integrated perspective across causing factors, outcomes, and governance: (a) (Poor) business-IT alignment, (b) (lack of) agility, and (c) (lack of) policies. These three category-spanning themes are potential starting points for researchers to provide an integrated perspective on Shadow IT and Business-managed IT instances across their whole lifecycle.

Third, governance approaches are still under-researched, even if they gained research attention in recent years (Klotz et al. [51]). General governance measures, such as policies, as well as governance measures for overt Business-managed IT instances, such as co-governance arrangements, are critical themes in practitioner perceptions but underrepresented in literature. Researchers can, for example, shed light on effective policy design for Business-managed IT. Besides, scholars could compare different forms of IT co-governance and development methodologies that consider tightly integrated teams consisting of IT and business employees.

Fourth, the different perceptions of all stakeholder groups, including IT managers (which were the focus of this study), business managers, IT users, and customers, should be investigated with integrated studies.

REFERENCES

[1] Ahuja, S. and Gallupe, B. "A Foundation for the Study of Personal Cloud Computing in Organizations," *Proceedings of the 21st Americas Conference on Information Systems*, Fajardo, 13-15 August 2015, pp. 1–12.

[2] Alter, S. "Theory of Workarounds," *Communications of the Association for Information Systems*, Volume 34, Number 1, 2014, pp. 1041–1066.

[3] Andriole, S.J. "Who Owns IT?," *Communications of the Association for Information Systems*, Volume 58, Number 3, 2015, pp. 50–57.

[4] Azad, B. and King, N. "Institutional Analysis of Persistent Computer Workarounds," *Proceedings of the Academy of Management*, Chicago, IL, 07-11 August 2009, pp. 1–41.

[5] Azad, B. and King, N. "Institutionalized Computer Workaround Practices in a Mediterranean Country: An Examination of Two Organizations," *European Journal of Information Systems*, Volume 21, Number 4, 2012, pp. 358–372.

[6] Behrens, S. "Shadow Systems: The Good, The Bad and The Ugly," *Communications of the Association for Information Systems*, Volume 52, Number 2, 2009, pp. 124–129.

[7] Behrens, S. and Sedera, W. "Why Do Shadow Systems Exist after an ERP Implementation? Lessons from a Case Study," *Proceedings of the 8th Pacific Asia Conference on Information Systems*, Shanghai, 08-11 July 2004, pp. 1713–1726.

[8] Beimborn, D. and Palitza, M. "Enterprise App Stores for Mobile Applications: Development of a Benefits Framework," *Proceedings of the 19th Americas Conference on Information Systems*, Chicago, IL, 15-17 August 2013, pp. 1–11.

[9] Benbasat, I., Goldstein, D.K. and Mead, M. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly*, Volume 11, Number 3, 1987, pp. 369–386.

[10] Berente, N., Yoo, Y. and Lyytinen, K. "Alignment or Drift: Loose Coupling over Time in NASA's ERP Implementation," *Proceedings of the 29th International Conference on Information Systems*, Paris, 14-17 December 2008, pp. 1–17.

[11] Bob-Jones, B., Newman, M. and Lyytinen, K. "Picking Up the Pieces After a "Successful" Implementation: Networks, Coalitions and ERP Systems," *Proceedings of the 14th Americas Conference on Information Systems*, Toronto, ON, 14-17 August 2008, pp. 1–12.

[12] Boudreau, M.-C. and Robey, D. "Enacting Integrated Information Technology: A Human Agency Perspective," *Organization Science*, Volume 16, Number 1, 2005, pp. 3–18.

[13] Buchwald, A. and Urbach, N. "Exploring the Role of Un-Enacted Projects in IT Project Portfolio Management," *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL, 16-19 December 2012, pp. 1–10.

[14] Buchwald, A. and Urbach, N. "Implikationen von inoffiziellen Projekten für die IT-Governance," *HMD Praxis der Wirtschaftsinformatik*, Volume 51, Number 3, 2014, pp. 319–329.

[15] Buchwald, A., Urbach, N. and Ahlemann, F. "Understanding the Organizational Antecedents of Bottom-up Un-enacted-Projects," *Proceedings of the 22nd European Conference on Information Systems*, Tel Aviv, 09-11 June 2014, pp. 1–16.

[16] Buchwald, A., Urbach, N. and Mähring, M. "Understanding Employee Engagement in Un-official Projects - A Conceptual Model Based on Psychological Empowerment and Constructive Deviance," *Proceedings of the 36th International Conference on Information Systems*, Fort Worth, TX, 13-16 December 2015, pp. 1–12.

[17] Bygstad, B. "Generative Innovation: A Comparison of Lightweight and Heavyweight IT," *Journal of Information Technology*, Volume 32, Number 2, 2017, pp. 180–193.

[18] Chua, C.E.H. and Storey, V.C. "Bottom-Up Enterprise Information Systems," *Communications of the Association for Information Systems*, Volume 60, Number 1, 2016, pp. 66–72.

[19] Chua, C.E.H., Storey, V.C. and Chen, L. "Central IT or Shadow IT? Factors Shaping Users' Decision to Go Rogue with IT," *Proceedings of the 35th International Conference on Information Systems*, Auckland, 14-17 December 2014, pp. 1–14.

[20] Corbin, J.M. and Strauss, A.L., *Basics of Qualitative Research. Techniques and Procedures for Developing Grounded Theory*, SAGE Publications, Los Angeles, CA, 2015.

[21] Corbin, K. "CIOs Vastly Underestimate Extent of Shadow IT," https://www.cio.com/article/2968281/cio-role/cios-vastly-underestimate-extent-of-shadow-it.html, 2015.

[22] Davison, R.M. and Ou, C.X.J. "Subverting Organisational IT Policy: A Case in China," *Proceedings of the 21st Americas Conference on Information Systems*, Fajardo, 13-15 August 2015, pp. 1–10.

[23] Davison, R.M., Ou, C.X.J. and Chang, Y. "Subverting Organisational IS Policy with Feral Systems: A Case in China," *Industrial Management & Data Systems*, Volume 118, Number 3, 2018, pp. 570–588.

[24] Dittes, S., Urbach, N., Ahlemann, F., Smolnik, S. and Müller, T. "Why Don't You Stick to Them? Understanding Factors Influencing and Counter-Measures to Combat Deviant Behavior Towards Organizational IT Standards," *Proceedings of the 12. Internationale Tagung Wirtschaftsinformatik*, Osnabrück, 04-06 March 2015, pp. 615–629.

[25] Ebeling, B., Köpp, C. and Breitner, M.H. "Diskussion eines Prototyps für das dezentrale Management von Forschungsressourcen an deutschen Hochschulinstituten," *Proceedings of the 11. Internationale Tagung Wirtschaftsinformatik*, Leipzig, 27 February - 01 March 2013, pp. 343–357.

[26] Ferneley, E.H. "Covert End User Development: A Study of Success," *Journal of Organizational and End User Computing*, Volume 19, Number 1, 2007, pp. 62–71.

[27] Ferneley, E.H. and Sobreperez, P. "Resist, Comply or Workaround? an Examination of Different Facets of User Engagement with Information Systems," *European Journal of Information Systems*, Volume 15, Number 4, 2006, pp. 345–356.

[28] Fürstenau, D. and Rothe, H. "Shadow IT Systemes: Discerning the Good and the Evil," *Proceedings of the 22nd European Conference on Information Systems*, Tel Aviv, 09-11 June 2014, pp. 1–14.

[29] Fürstenau, D., Rothe, H. and Sandner, M. "Shadow Systems, Risk, and Shifting Power Relations in Organizations," *Communications of the Association for Information Systems*, Volume 41, 2017, pp. 43–61.

[30] Fürstenau, D., Rothe, H. and Sandner, M. "Leaving the Shadow: A Configurational Approach to Explain Post-Identification Outcomes of Shadow It Systems," *Business & Information Systems Engineering*, 2020.

[31] Fürstenau, D., Rothe, H., Sandner, M. and Anapliotis, D. "Shadow IT, Risk, and Shifting Power Relations in Organizations," *Proceedings of the 22nd Americas Conference on Information Systems*, San Diego, CA, 11-13 August 2016, pp. 1–10.

[32] Fürstenau, D., Sandner, M. and Anapliotis, D. "Why do Shadow Systems Fail? An Expert Study on Determinants of Discontinuation," *Proceedings of the 24th European Conference on Information Systems*, Istanbul, 12-15 June 2016, pp. 1–16.

[33] Gartner "Make the Best of Shadow IT," https://www.gartner.com/smarterwithgartner/make-the-best-of-shadow-it/, 2017.

[34] Gozman, D. and Willcocks, L.P. "Crocodiles in the Regulatory Swamp: Navigating the Dangers of Outsourcing, SaaS and Shadow IT," *Proceedings of the 36th International Conference on Information Systems*, Fort Worth, TX, 13-16 December 2015, pp. 1–20.

[35] Györy, A., Cleven, A., Uebernickel, F. and Brenner, W. "Exploring the Shadows: IT Governance Approaches to User-driven Innovation," *Proceedings of the 20th European Conference on Information Systems*, Barcelona, 11-13 June 2012, pp. 1–12.

[36] Haag, S. "Appearance of Dark Clouds? – An Empirical Analysis of Users' Shadow Sourcing of Cloud Services," *Proceedings of the 12. Internationale Tagung Wirtschaftsinformatik*, Osnabrück, 04-06 March 2015, pp. 1438–1452.

[37] Haag, S. and Eckhardt, A. "Normalizing the Shadows – The Role of Symbolic Models for Individuals' Shadow IT Usage," *Proceedings of the 35th International Conference on Information Systems*, Auckland, 14-17 December 2014, pp. 1–13.

[38] Haag, S. and Eckhardt, A. "Sensitizing Employees' Corporate IS Security Risk Perception," *Proceedings of the 35th International Conference on Information Systems*, Auckland, 14-17 December 2014, pp. 1–17.

[39] Haag, S. and Eckhardt, A. "Justifying Shadow IT Usage," *Proceedings of the 19th Pacific Asia Conference on Information Systems*, Singapore, 05-09 July 2015, pp. 1–11.

[40] Haag, S. and Eckhardt, A. "Shadow IT," *Business & Information Systems Engineering*, Volume 59, Number 6, 2017, pp. 469–473.

[41] Haag, S., Eckhardt, A. and Bozoyan, C. "Are Shadow System Users the Better IS Users? – Insights of a Lab Experiment," *Proceedings of the 36th Inter-*

national Conference on Information Systems, Fort Worth, TX, 13-16 December 2015, pp. 1–20.

[42] Hetzenecker, J., Sprenger, S., Kammerer, S. and Amberg, M. "The Unperceived Boon and Bane of Cloud Computing: End-User Computing vs. Integration," *Proceedings of the 18th Americas Conference on Information Systems*, Seattle, WA, 9-12 August 2012, pp. 1–9.

[43] Houghton, L. and Kerr, D.V. "A Study into the Creation of Feral Information Systems as a Response to an ERP Implementation Within the Supply Chain of a Large Government-Owned Corporation," *International Journal of Internet & Enterprise Management*, Volume 4, Number 2, 2006, pp. 135–147.

[44] Huber, M., Zimmermann, S., Rentrop, C. and Felden, C. "Integration of Shadow IT Systems with Enterprise Systems - A Literature Review," *Proceedings of the 21st Pacific Asia Conference on Information Systems,* Langkawi, 16-20 July 2017, pp. 1–12.

[45] Huber, M., Zimmermann, S., Rentrop, C. and Felden, C. "The Influence of Shadow IT Systems on Enterprise Architecture Management Concerns," *Proceedings of the European, Mediterranean, and Middle Eastern Conference on Information Systems,* Coimbra, 07-08 September 2017, pp. 461–477.

[46] Huuskonen, S. and Vakkari, P. "“I Did It My Way”: Social Workers as Secondary Designers of a Client Information System," *Information Processing & Management*, Volume 49, Number 1, 2013, pp. 380–391.

[47] Jones, D., Behrens, S., Jamieson, K. and Tansley, E. "The Rise and Fall of a Shadow System: Lessons for Enterprise System Implementation," *Proceedings of the 15th Australasian Conference on Information Systems,* Hobart, 01-03 December 2004, pp. 1–14.

[48] Kerr, D.V., Houghton, L. and Burgess, K. "Power Relationships that Lead to the Development of Feral Systems," *Australasian Journal of Information Systems,* Volume 14, Number 2, 2007, pp. 141–152.

[49] Khalil, S., Winkler, T.J. and Xiao, X. "Two Tales of Technology: Business and IT Managers’ Technological Frames Related to Cloud Computing," *Proceedings of the 38th International Conference on Information Systems,* Seoul, 10-13 December 2017, pp. 1–20.

[50] Klotz, S. "Shadow IT and Business-Managed IT: Where Is the Theory?," *2019 IEEE 21st Conference on Business Informatics (CBI),* Moscow, 7/15/2019 - 7/17/2019, pp. 286–295.

[51] Klotz, S., Kopper, A., Westner, M. and Strahringer, S. "Causing Factors, Outcomes, and Governance of Shadow IT and Business-managed IT: A Systematic Literature Review," *International Journal of Information Systems and Project Management*, Volume 7, Number 1, 2019, pp. 15–43.

[52] Köffer, S., Ortbach, K., Junglas, I., Niehaves, B. and Harris, J. "Innovation Through BYOD?: The Influence of IT Consumerization on Individual IT Innovation Behavior," *Business & Information Systems Engineering*, Volume 57, Number 6, 2015, pp. 363–375.

[53] Koopman, P. and Hoffman, R.R. "Work-Arounds, Make-Work, and Kludges," *IEEE Intelligent Systems,* Volume 18, Number 6, 2003, pp. 70–75.

[54] Kopper, A. "Perceptions of IT Managers on Shadow IT," *Proceedings of the 23rd Americas Conference on Information Systems,* Boston, MA, 10-12 August 2017, pp. 1–10.

[55] Kopper, A., Fürstenau, D., Zimmermann, S., Klotz, S., Rentrop, C., Rothe, H., Strahringer, S. and Westner, M. "Shadow IT and Business-Managed IT: A Conceptual Framework and Empirical Illustration," *International Journal of IT/Business Alignment and Governance*, Volume 9, Number 2, 2018, pp. 53–71.

[56] Kopper, A., Fürstenau, D., Zimmermann, S., Rentrop, C., Rothe, H., Strahringer, S. and Westner, M. "Business-managed IT: A Conceptual Framework and Empirical Illustration," *Proceedings of the 26th European Conference on Information Systems,* Portsmouth, 23-28 June 2018, pp. 1–16.

[57] Kopper, A. and Westner, M. "Deriving a Framework for Causes, Consequences, and Governance of Shadow IT from Literature," *Proceedings of the Multikonferenz Wirtschaftsinformatik,* Ilmenau, 09-11 March 2016, pp. 1687–1698.

[58] Kopper, A., Westner, M. and Strahringer, S. "Kontrollierte Nutzung von Schatten-IT," *HMD Praxis der Wirtschaftsinformatik,* Volume 54, Number 1, 2017, pp. 97–110.

[59] Kretzer, M. "Linking Report Individualization and Report Standardization: A Configurational Perspective," *Proceedings of the 23rd European Conference on Information Systems,* Münster, 26-29 May 2015, pp. 1–18.

[60] Kretzer, M. and Maedche, A. "Generativity of Business Intelligence Platforms: A Research Agenda Guided by Lessons from Shadow IT," *Proceedings of the Multikonferenz Wirtschaftsinformatik,* Paderborn, 26-28 February 2014, pp. 208–220.

[61] Luftman, J. "Assessing Business-IT Alignment Maturity," *Communications of the Association for Information Systems*, Volume 4, 2000, pp. 1–50.

[62] Lund-Jensen, R., Azaria, C., Permien, F.H., Sawari, J. and Bækgaard, L. "Feral Information Systems, Shadow Systems, and Workarounds: A Drift in IS Terminology," *Procedia Computer Science*, Volume 100, 2016, pp. 1056–1063.

[63] Lyytinen, K. and Newman, M. "A Tale of Two Coalitions - Marginalising the Users While Successfully Implementing an Enterprise Resource Planning System," *Information Systems Journal*, Volume 25, Number 2, 2015, pp. 71–101.

[64] Mallmann, G.L. and Maçada, A.C.G. "Behavioral Drivers Behind Shadow IT and Its Outcomes in Terms of Individual Performance," *Proceedings of the 22nd Americas Conference on Information Systems*, San Diego, CA, 11-13 August 2016, pp. 1–5.

[65] Mallmann, G.L. and Maçada, A.C.G. "The Mediating Role of Social Presence on the Relationship between Shadow IT Usage and Individual Performance: A Social Presence Theory Perspective," *Proceedings of the VI Encontro de Administração da Informação*, 28-30 May 2017, pp. 1–9.

[66] Mallmann, G.L., Maçada, A.C.G. and Oliveira, M. "Can Shadow IT Facilitate Knowledge Sharing in Organizations? An Exploratory Study," *Proceedings of the 17th European Conference on Knowledge Management*, Belfast, 11-18 February 2016, pp. 1–10.

[67] Mallmann, G.L., Maçada, A.C.G. and Oliveira, M. "The Influence of Shadow IT Usage on Knowledge Sharing: An Exploratory Study with IT Users," *Business Information Review*, Volume 35, Number 1, 2018, pp. 17–28.

[68] Marrone, M. and Hammerle, M. "Relevant Research Areas in IT Service Management: An Examination of Academic and Practitioner Literatures," *Communications of the Association for Information Systems*, Volume 41, 2017, pp. 517–543.

[69] McCoy, C. and Rosenbaum, H. "Uncovering Unintended and Shadow Practices of Users of Decision Support System Dashboards in Higher Education Institutions," *Journal of the Association for Information Science and Technology*, Volume 70, Number 4, 2019, pp. 370–384.

[70] McGill, T.J. "The Effect of End User Development on End User Success," *Journal of Organizational and End User Computing*, Volume 16, Number 1, 2004, pp. 41–58.

[71] Melo, C.d.O., Moraes, J., Ferreira, M. and Figueiredo, Rejane Maria da Costa "A Method for Evaluating End-User Development Technologies," *Proceedings of the 23rd Americas Conference on Information Systems*, Boston, MA, 10-12 August 2017, pp. 1–10.

[72] Mokosch, G., Niehaves, B. and Klesel, M. "Putting Flesh on the Duality of Structure: The Case of IT Consumerization," *Proceedings of the 21st Americas Conference on Information Systems*, Fajardo, 13-15 August 2015, pp. 1–10.

[73] Myers, M.D. and Newman, M. "The Qualitative Interview in IS Research: Examining the Craft," *Information and Organization*, Volume 17, Number 1, 2007, pp. 2–26.

[74] Ologeanu-Taddei, R., Wessel, L. and Bourdon, I. "Persistent Paradoxes in Pluralistic Organizations: A Case Study of Continued Use of Shadow-IT in a French Hospital," *Proceedings of the 40th International Conference on Information Systems*, Munich, 15-18 December 2019.

[75] Ortbach, K., Bode, M. and Niehaves, B. "What Influences Technological Individualization? - An Analysis of Antecedents to IT Consumerization Behavior," *Proceedings of the 19th Americas Conference on Information Systems*, Chicago, IL, 15-17 August 2013, pp. 1–9.

[76] Ortbach, K., Köffer, S., Bode, M. and Niehaves, B. "Individualization of Information Systems - Analyzing Antecedents of IT Consumerization Behavior," *Proceedings of the 34th International Conference on Information Systems*, Milan, 13-15 December 2013, pp. 1–18.

[77] Pan, S.L. and Tan, B. "Demystifying Case Research: A Structured–Pragmatic–Situational (SPS) Approach to Conducting Case Studies," *Information and Organization*, Volume 21, Number 3, 2011, pp. 161–176.

[78] Panko, R.R. and Port, D.N. "End User Computing: The Dark Matter (and Dark Energy) of Corporate IT," *Proceedings of the 45th Hawaii International Conference on System Sciences*, Maui, HI, 04-07 January 2012, pp. 4603–4612.

[79] Peppard, J. "The Application of the Viable Systems Model to Information Technology Governance," *Proceedings of the 26th International Conference on Information Systems*, Las Vegas, NV, 11-14 December 2005, pp. 45–58.

[80] Raković, L. "A Framework for Managing Spreadsheet-Based End User Applications," *International Journal of Management and Decision Making*, Volume 18, Number 1, 2019, p. 76.

[81] Ramiller, N. and Pentland, B. "Management Implications in Information Systems Research: The Untold Story," *Journal of the Association for Infor-*

mation Systems, Volume 10, Number 6, 2009, pp. 474–494.

[82] Rentrop, C. and Zimmermann, S. "Shadow IT: Management and Control of unofficial IT," *Proceedings of the 6th International Conference on Digital Society,* Valencia, 30 January - 04 February 2012, 98–102.

[83] Rentrop, C. and Zimmermann, S. "Shadow IT Evaluation Model," *Proceedings of the Federated Conference on Computer Science and Information Systems,* Wroclaw, 9-12 September 2012, pp. 1023–1027.

[84] Rentrop, C., Zimmermann, S. and Huber, M. "Schatten-IT – ein unterschätztes Risiko?," *Proceedings of the D·A·CH Security Conference*, pp. 291–300.

[85] Röder, N., Wiesche, M. and Schermann, M. "A Situational Perspective on Workarounds in IT-enabled Business Processes: A Multiple Case Study," *Proceedings of the 22nd European Conference on Information Systems,* Tel Aviv, 09-11 June 2014, pp. 1–15.

[86] Röder, N., Wiesche, M., Schermann, M. and Krcmar, H. "Toward an Ontology of Workarounds: A Literature Review on Existing Concepts," *Proceedings of the 49th Hawaii International Conference on System Sciences,* Koloa, HI, 05-08 January 2016, pp. 5177–5186.

[87] Schalow, P.R., Winkler, T.J., Repschläger, J. and Zarnekow, R. "The Blurring Boundaries of Work-related and Personal Media Use: A Grounded Theory Study on the Employee's Perspective," *Proceedings of the 21st European Conference on Information Systems*, Utrecht, 06-08 June 2013, pp. 1–12.

[88] Segal, M. "Dealing with the Realities of Shadow IT," http://www.datacenterjournal.com/dealing-realities-shadow, 2016.

[89] Silic, M. "Critical Impact of Organizational and Individual Inertia in Explaining Non-Compliant Security Behavior in the Shadow IT Context," *Computers & Security*, Volume 80, 2019, pp. 108–119.

[90] Silic, M. and Back, A. "Shadow IT – A View from Behind the Curtain," *Computers & Security*, Volume 45, 2014, pp. 274–283.

[91] Silic, M., Barlow, J.B. and Back, A. "A New Perspective on Neutralization and Deterrence: Predicting Shadow IT Usage," *Information & Management*, Volume 54, Number 8, 2017, pp. 1023–1037.

[92] Silic, M., Silic, D. and Oblakovic, G. "Influence of Shadow IT on Innovation in Organizations," *Complex Systems Informatics and Modeling Quarterly, Number* 8, 2016, pp. 68–80.

[93] Silva, L. and Fulk, H.K. "From Disruptions to Struggles: Theorizing Power in ERP Implementation Projects," *Information and Organization*, Volume 22, Number 4, 2012, pp. 227–251.

[94] Singh, H. "Emergence and Consequences of Drift in Organizational Information Systems," *Proceedings of the 19th Pacific Asia Conference on Information Systems,* Singapore, 05-09 July 2015, pp. 1–15.

[95] Spierings, A., Kerr, D.V. and Houghton, L. "What Drives the End User to Build a Feral Information System?," *Proceedings of the 23rd Australasian Conference on Information Systems,* Geelong, 03-05 December 2012, pp. 1–10.

[96] Spierings, A., Kerr, D.V. and Houghton, L. "Issues That Support the Creation of ICT Workarounds: Towards a Theoretical Understanding of Feral Information Systems," *Information Systems Journal*, Volume 27, Number 6, 2017, pp. 775–794.

[97] Steinhüser, M., Waizenegger, L., Vodanovich, S. and Richter, A. "Knowledge Management without Management - Shadow IT in Knowledge-Intensive Manufacturing Practices," *Proceedings of the 25th European Conference on Information Systems,* Guimarães, 05-10 June 2017, pp. 1647–1662.

[98] Tambo, T. and Bækgaard, L. "Dilemmas in Enterprise Architecture Research and Practice from a Perspective of Feral Information Systems," *Proceedings of the 17th IEEE International Enterprise Distributed Object Computing Conference Workshops,* Vancouver, BC, 09-13 September 2013, pp. 289–295.

[99] Thatte, S., Grainger, N. and McKay, J. "Feral Practices," *Proceedings of the 23rd Australasian Conference on Information Systems,* Geelong, 03-05 December 2012, pp. 1–10.

[100] vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R. and Cleven, A. "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," *Proceedings of the 17th European Conference on Information Systems*, Verona, 8-10 June 2009, pp. 1–12.

[101] Walterbusch, M., Fietz, A. and Teuteberg, F. "Schatten-IT: Implikationen und Handlungsempfehlungen für Mobile Security," *HMD Praxis der Wirtschaftsinformatik*, Volume 51, Number 1, 2014, pp. 24–33.

[102] Walterbusch, M., Fietz, A. and Teuteberg, F. "Missing Cloud Security Awareness: Investigating Risk Exposure in Shadow IT," *Journal of Enterprise Information Management*, Volume 30, Number 4, 2017, pp. 644–665.

[103] Walters, R. "Bringing IT out of the Shadows," *Network Security*, Volume 2013, Number 4, 2013, pp. 5–11.

[104] Webster, J. and Watson, R.T. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, Volume 26, Number 2, 2002, pp. xiii–xxiii.

[105] Winkler, T.J. and Brown, C.V. "Horizontal Allocation of Decision Rights for On-Premise Applications and Software-as-a-Service," *Journal of Management Information Systems*, Volume 30, Number 3, 2013, pp. 13–48.

[106] Yin, R.K., *Case Study Research. Design and Methods*, SAGE Publications, Thousand Oaks, CA, 2013.

[107] Zainuddin, E. "Secretly SaaS-ing: Stealth Adoption of Software-as-a-Service from the Embeddedness Perspective," *Proceedings of the 33rd International Conference on Information Systems*, Orlando, FL, 16-19 December 2012, pp. 1–10.

[108] Zimmermann, S. and Rentrop, C. "Schatten-IT," *HMD Praxis der Wirtschaftsinformatik*, Volume 49, Number 6, 2012, pp. 60–68.

[109] Zimmermann, S. and Rentrop, C. "On the Emergence of Shadow IT - A Transaction Cost-based Approach," *Proceedings of the 22nd European Conference on Information Systems*, Tel Aviv, 09-11 June 2014, pp. 1–17.

[110] Zimmermann, S., Rentrop, C. and Felden, C. "Managing Shadow IT Instances – A Method to Control Autonomous IT Solutions in the Business Departments," *Proceedings of the 20th Americas Conference on Information Systems*, Savannah, GA, 07-09 August 2014, pp. 1–12.

[111] Zimmermann, S., Rentrop, C. and Felden, C. "Governing IT Activities in Business Workgroups—Design Principles for a Method to Control Identified Shadow IT," *Business Information Systems*, Leipzig, 06-08 July 2016, pp. 252–264.

[112] Zimmermann, S., Rentrop, C. and Felden, C. "Governing Identified Shadow IT by Allocating IT Task Responsibilities," *Proceedings of the 22nd Americas Conference on Information Systems*, San Diego, CA, 11-13 August 2016, pp. 1–10.

[113] Zimmermann, S., Rentrop, C. and Felden, C. "A Multiple Case Study on the Nature and Management of Shadow Information Technology," *Journal of Information Systems*, Volume 31, Number 1, 2017, pp. 79–101.

AUTHOR BIOGRAPHIES

Andreas Kopper obtained a PhD from the Faculty of Business and Economics at TU Dresden, Germany. He graduated from the TU Wien with a master’s degree in Information Systems. His research interests focus on Shadow IT and IS managed in business units. In this field, he has published several journal articles and conference papers at the AMCIS, ECIS, MWKI, and HMD Praxis der Wirtschaftsinformatik, among others. His doctoral thesis was about Shadow IT and Business-managed IT.

Stefan Klotz is a PhD candidate at the Faculty of Business and Economics TU Dresden, Germany. He graduated from the Technical University of Munich and the University of Augsburg with a master’s degree in Finance and Information Management. His research interests focus on IS governance and IS managed in business units, and he is writing his doctoral thesis about Business-managed IT and IT governance.

Markus Westner is a professor of IT Management at OTH Regensburg, Germany. He is author of several journal articles and conference papers. His work focuses on IT strategy and IT sourcing. He acts as an Associate Editor for Information & Management. He has served as a reviewer for the ACIS, AMCIS, BISE, CAIS, ECIS, HMD, JoCCASA, MKWI, and WI. Before he started his academic career, he worked as a management consultant in a project manager position for one of the world’s largest management consultancies.

Susanne Strahringer is a professor of Business Information Systems, especially IS in Manufacturing and Commerce at TU Dresden, Germany. Before joining TU Dresden, she held positions at the University of Augsburg and the European Business School. She graduated from the Darmstadt University of Technology, where she also obtained her PhD and completed her habilitation thesis. She has published in Information & Management, Journal of Information Technology Theory and Application, Information Systems Management, and Journal of Information Systems Education, among others. Her research interests focus on IS management, ERP systems, and enterprise modeling.