Causing factors, outcomes, and governance of Shadow IT and business-managed IT: a systematic literature review

Stefan Klotz
TU Dresden
Helmholtzstr. 10, 01069 Dresden, Germany
www.shortbio.org/stefan.klotz1@mailbox.tu-dresden.de

Markus Westner
OTH Regensburg
Galgenbergstr. 32, 93053 Regensburg, Germany
www.shortbio.org/markus.westner@oth-regensburg.de

Andreas Kopper
TU Dresden
Helmholtzstr. 10, 01069 Dresden, Germany
www.shortbio.org/andreas.kopper@mailbox.tu-dresden.de

Susanne Strahringer
TU Dresden
Helmholtzstr. 10, 01069 Dresden, Germany
www.shortbio.org/susanne.strahringer@tu-dresden.de

Abstract:
Shadow IT and Business-managed IT describe the autonomous deployment/procurement or management of Information Technology (IT) instances, i.e., software, hardware, or IT services, by business entities. For Shadow IT, this happens covertly, i.e., without alignment with the IT organization; for Business-managed IT this happens overtly, i.e., in alignment with the IT organization or in a split responsibility model. We conduct a systematic literature review and structure the identified research themes in a framework of causing factors, outcomes, and governance. As causing factors, we identify enablers, motivators, and missing barriers. Outcomes can be benefits as well as risks/shortcomings of Shadow IT and Business-managed IT. Concerning governance, we distinguish two subcategories: general governance for Shadow IT and Business-managed IT and instance governance for overt Business-managed IT. Thus, a specific set of governance approaches exists for Business-managed IT that cannot be applied to Shadow IT due to its covert nature. Hence, we extend the existing conceptual understanding and allocate research themes to Shadow IT, Business-managed IT, or both concepts and particularly distinguish the governance of the two concepts. Besides, we find that governance themes have been the primary research focus since 2016, whereas older publications (until 2015) focused on causing factors.

1. Introduction

Shadow IT and Business-managed IT describe the autonomous deployment/procurement or management of Information Technology (IT) by business units (BUs). The term BU refers to all types of business entities (e.g., individual users, business workgroups, departments, or divisions) and is subsequently used for the purpose of simplification [1]. Shadow IT happens covertly [2]; that is, IT instances—software, hardware, or IT services— are created/procured or managed by BUs without alignment with the IT organization [1, 3]. The term IT organization refers to internal IT organizations, e.g., company-internal IT departments. In contrast, the concept Business-managed IT refers to autonomous and open deployment/procurement or management of information systems (IS) by BUs in alignment with the IT organization or in a split responsibility model [1, 3]. Recent surveys show that Shadow IT is a widespread phenomenon: Kopper [4] finds that 80% of employees use software that has not been approved by the IT organization. However, the true extent of Shadow IT usage in companies is vastly underestimated by CIOs [5], even though Shadow IT is gaining increased research attention [6].

Currently, there is a lack of research that clearly distinguishes and separates Shadow IT and Business-managed IT, which impedes the discussion of specific IT governance issues in organizations [1]. Accordingly, a systematic literature review improves differentiation between the two concepts, provides valuable insights, and creates a basis for further research targeting the two concepts. In order to approach this research gap, the paper at hand provides a systematic literature review of the scientific literature on Shadow IT and Business-managed IT. We, therefore, pose the following research question: *Which themes exist in research on Shadow IT, Business-managed IT, and related concepts, and how can these research themes be categorized?*

In order to address this research question, we conducted a rigorous review of 107 scientific literature items. We categorized research themes according to causing factors, outcomes, and governance, and we present these research themes in a comprehensive framework. Hence, this paper creates transparency about the research themes within the developing research field of Shadow IT and Business-managed IT. Consequently, researchers can build on this framework and address identified gaps in the current research.

The remainder of the paper is organized as follows: Section 2 conceptualizes Shadow IT and Business-managed IT through an extended taxonomy and provides an overview of literature reviews in the research field. This is followed by a methodology overview in section 3, including the scope of this literature review, and the literature search, selection, and extraction. In section 4, we present the results of the literature review and introduce a framework to categorize the identified research themes as causing factors, outcomes, or governance. Additionally, this section provides a longitudinal analysis of the research focuses to date. Section 5 discusses the identified research themes for Shadow IT and Business-managed IT as well as specific governance recommendations. The paper then concludes with a summary of the results and limitations of this study as well as avenues for further research.

2. Background

2.1 Conceptualization

Kopper and Westner [7] provide a taxonomy for Shadow IT and the following five related concepts: Feral Practices, Workarounds, Shadow Systems, Un-enacted Projects, and Shadow Sourcing. Figure 1 illustrates this taxonomy and extends it. In the taxonomy defined in Kopper and Westner [7], five dimensions, with two characteristics each, are used to differentiate the related concepts:

- (a) Novelty: Unofficial IT, misuse of official IT;

- (b) Perspective: Creation, outcome;

- (c) Artifact: Devices, applications;

- ▪ (d) Infrastructure: Shadow infrastructure, official infrastructures;

- ▪ (e) Scale: Group, individual.

For precise definitions of these five dimensions and their associated characteristics, please refer to Kopper and Westner [7, p. 3]. Furthermore, Kopper and Westner [7] categorize Shadow IT as (a) unofficial IT, (b) outcome, (c) devices & applications, (d) shadow & official infrastructure, and (e) group & individual. In the paper at hand, we conceptualize Shadow IT as software, hardware, or IT services created or used by BUs without alignment with or awareness of the IT organization [1, 7, 8]. Hence, Shadow IT is *covert* [2, 9]*; that is, IS activities are practiced in a hidden form [1, 10].

Furthermore, Kopper et al. [1] introduce the term *Business-managed IT* for IS for which the IT task responsibility [11, 12] resides in the BU. This characteristic is shared with Shadow IT; however, in contrast to Shadow IT, Business-managed IT is *overt* [9]. Hence, "the term 'Business-managed IT' describe[s] 'overt' information systems developed or managed by business entities" [1, p. 1]. In conclusion, the involvement in the organizational IT management is the main distinction between Shadow IT (IT instances are covert and thus "in the shadows" [1, p. 1]) and Business-managed IT (IT instances are overt [1]). In order to accommodate for Business-managed IT, we extend the taxonomy of Kopper and Westner [7] and add the characteristic *official IT* to dimension (a) novelty. Business-managed IT is, by definition, based on (d) official infrastructure, whereas Shadow IT uses shadow & official infrastructure. Business-managed IT and Shadow IT share the same characteristics of the three remaining dimensions: Business-managed IT is outcome-oriented ((b) perspective), it includes devices and applications ((c) artifact), and it can occur at group & individual level ((e) scale). Figure 1 provides a visualization of the extended taxonomy.
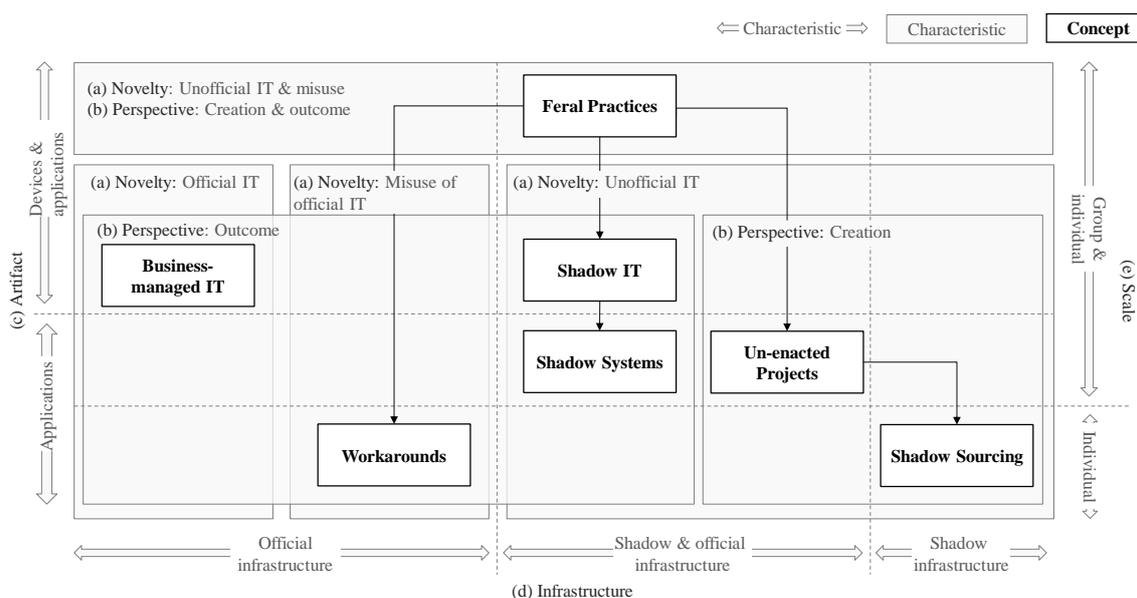

Figure 1: Extended taxonomy based on Kopper and Westner [7, p. 4]

2.2 Related works

In recent years, several literature reviews have been conducted on Shadow IT and related concepts; Table 1 provides an overview of these reviews. Most of the reviews target specific concepts of this research field or related fields. Almost all existing reviews analyze the scientific literature (i.e., scientific journal papers or papers in scientific conference proceedings); nevertheless, practitioner literature (i.e., white papers or internet articles targeting practitioners as audience) are also reviewed in a few existing publications.

Table 1. Overview of existing literature reviews and their targeted concepts as classified in the extended taxonomy (see Figure 1)

Source	Targeted concepts of extended taxonomy	Analyzed time-frame	Lit. search and selection	Types of sources	No. incl. lit. items	No. ident. research themes	Framework for research themes
[15]	Focused on workarounds	1967–2013	Search process vague	Scientific literature	300+	37	Phenomena associated with workarounds, types of workarounds, direct effects of workarounds, perspectives of workarounds, organizational challenges and dilemmas related to workarounds
[16]	Focused on Shadow IT	Until 02/2017	Rigorous	Scientific literature	45	41	Concerns associated with technology homogeneity, application landscape planning, support of business processes, project portfolio management, infrastructure management, interface, business object and service management
[17]	Focused on Shadow IT and Business-managed IT	Until 12/2016	Rigorous	Scientific literature	52	34	Five phases of Shadow IT integration: Terminology, pre-integration, integration decision, integration process, post-integration
[13]	Concept-overarching, incl. Feral Practices, Workarounds, Shadow IT, Shadow Systems, Un-enacted Projects, and Shadow Sourcing	2010–2015	Rigorous	Scientific literature	52	22	Causes, consequences, governance of Shadow IT
[18]	Focused on Shadow IT, Business-managed IT	09/2015–08/2016	Rigorous	Practitioner literature	397	10	Pressure on IT, consequences for IT, controlled use of business-managed IT, realignment of IT
[19]	Focused on Shadow IT	Until 04/2013	Rigorous	Scientific literature	21	25	Benefits of Shadow IT, downsides of Shadow IT
[20]	Focused on Shadow IT and Workarounds	1997–2016	Search process vague	Scientific & practitioner literature	43	n/a	Two dimensions of phenomena: short term/long term, technology/process
[14]	Concept-overarching, incl. Feral Practices, Workarounds, Shadow IT, Shadow Systems, Un-enacted Projects, and Shadow Sourcing	2006–2017	Rigorous	Scientific literature	70	4	Causes of Shadow IT, benefits of Shadow IT, risks of Shadow IT; internal controls
[21]	Focused on Workarounds	1987–2011	Search process not defined	Scientific & practitioner literature	Not explicit	n/a	n/a
[22]	Focused on Workarounds	1986–2014	Rigorous	Scientific literature	84	n/a	Organizational goal, information system, social climate, rule; working environment, organizational member, conflict neutralization, resistance, workaround, risks, benefits
[23]	Focused on Feral Practices	Not explicit	Search process not defined	Scientific literature	Not explicit	n/a	Organizational structure, social influences, technological influences, structural strain, supporting factor, deviance in the form of Feral Practice

The reviews by Kopper and Westner [13] and Magunduni and Chigona [14] provide foundational literature reviews that cover most of the concepts of the research field. However, none of the existing reviews cover the research field completely, that is, including all seven concepts as outlined in Figure 1. Consequently, a systematic literature review, which structures the body of research covering the concepts of Shadow IT and Business-managed IT, is missing. The article at hand closes this gap and differentiates between the research themes of Shadow IT and Business-managed IT.

3. Methodology

3.1 Review scope

We adapted the approaches proposed by Levy and Ellis [24], Okoli [25], and vom Brocke [26] in order to conduct a rigorous, systematic, and comprehensive review of the scientific literature [25–28]. To define the scope of this review and to position this paper's focus, goal, perspective, coverage, organization, and audience, we use the taxonomy developed by Cooper [29] and Cooper and Hedges [30], which was later adapted by vom Brocke [26]. It is often used in IS research, as in the papers by Herz et al. [31], Kopper and Westner [13], or Strasser and Westner [32]. The classification used in this literature review, along with the taxonomy, is shown in Table 2. We focus on research outcomes, research methods, and theories. The goal of this literature review is to integrate related research, aggregate it into themes, and describe central issues. Our literature review groups research themes based on a conceptual view. We maintain a neutral perspective "attempt[ing] to present all arguments or evidence for and against various interpretations of the problem" [30, p. 5]. As its audience, the review addresses specialized scholars, general scholars, and practitioners. Furthermore, it aims to exhaustively cover the relevant literature, enabling synthesis and discussions on a comprehensive basis.

Table 2. Classification of literature review along taxonomy developed by Cooper [29, p. 109] and Cooper and Hedges [30, p. 5], later adapted by vom Brocke [26, p. 8]; shaded cells illustrating the paper's classifications

Characteristics	Categories			
Focus	Research outcomes	Research methods	Theories	Applications
Goal	Integration	Criticism	Central issues	
Organization	Historical	Conceptual	Methodological	
Perspective	Neutral representation		Espousal of position	
Audience	Specialized scholars	General scholars	Practitioners	General public
Coverage	Exhaustive	Exhaustive and selective	Representative	Central/pivotal

3.2 Literature search and selection

We followed a three-step approach for the systematic literature search [33]. First, we conducted a database search [24] for references published between January 2000 and August 2018, which also ensures comparability with Kopper and Westner [13]. We limited the database search to peer-reviewed journal articles as well as the proceedings of major IS conferences [24, 28], and queried the AIS Electronic Library, Business Source Complete (EBSCO), Emerald Insight, IEEE Xplore, ScienceDirect (Elsevier), and SpringerLink. For our keyword set, we applied two approaches: (1) we combined the keywords: "shadow," "feral," "workaround," "un-enacted," "unsanctioned," "rogue," and "grey" with "IT," "systems," and "projects." We also (2) searched for "bottom-up IT," "Business-managed IT," "end-user

development," and "user-driven innovation" to cover all concepts of the research field (see Figure 1). We applied the set of keywords to title, abstract, and keywords [28, 29]. Second, we conducted a practicality screening of the identified results to separate non-relevant publications based on an evaluation of title, abstract, and keywords [34]. We limited the results of SpringerLink to the two disciplines potentially relevant for Shadow IT and Business-managed IT: "Computer Science" and "Business Management." Third, we performed forward and backward searches for authors and references [24, 26, 33] in order to ensure an exhaustive search [25, 34]. We used Google Scholar for the forward search [25, 28, 35]. The results of the literature search and selection are shown in Table 3.

Table 3. Search and selection results as the number of resulting literature items

Type	Database/search step	Comments	No. of results	No. of relevant results	No. of duplicates
Journals	Business Source Complete (EBSCO)	-	109	15	
	Emerald Insight	-	238	2	1
	IEEE Xplore	-	70	0	0
	ScienceDirect (Elsevier)	-	353	4	3
	SpringerLink	Limited to disciplines "Computer Science" and "Business Management"	214	6	
Conference contributions	AIS Electronic Library	ACIS, AMCIS, ECIS, ICIS, PACIS proceedings; HICSS proceedings (since 2016 accessible via the AIS Electronic Library)	148	25	
	IEEE Xplore	HICSS proceedings (accessible via IEEE until 2016)	0	0	
Forward/ backward search	Forward/backward author search	-	n/a	8	
	Forward/backward reference search		n/a	51	
		Total		**111**	**4**
		Total relevant literature items after deduplication		**107**	

Through these three steps, we identified a total of 107 relevant literature items after deduplication, 50 (47%) via database search and 57 (53%) via forward/backward reference and author search. Most of the relevant literature items appeared in conference proceedings (67; 63%), namely at AMCIS (15; 22%), ECIS (13; 19%), ICIS (12; 18%), PACIS (4; 6%), and ACIS (4, 6%). The remaining literature items (40; 37%) are journal articles appearing, for example, in the Communications of the Association for Information Systems (6; 15%). The remaining conference contributions (19; 28%) are distributed across 15 conferences and the remaining journal articles (34; 85%) across 25 further periodicals.

Most of the literature items were published since 2012. That is, 10 to 17 articles/contributions were published in the years since 2012 (7 until August 2018). In contrast, between 2003 and 2009, only a few articles were published each year (1 to 4). Figure 2 illustrates that Shadow IT and Business-managed IT has been attracting high and increasing research attention since 2012. Moreover, 35% of the literature was published since 2016; thus, this literature review provides further insight complementing previous reviews, for example, Kopper and Westner [13].

3.3 Extraction

In order to describe the research setup used in the literature items, we built on the research designs outlined by Creswell [36] that are commonly used in literature reviews, as in Stödberg [37], and particularly in IS literature reviews, as in Jalali and Wohlin [38] and Kopper and Westner [13]. Consequently, we coded the philosophical worldview, research design, research approach, and data gathering method of every literature item. Aditionally, we examined data analysis methods as well as the number of data points evaluated—i.e., the number of case interviews, cases, and quantitative datasets—if applicable. Most literature items espouse a constructivist worldview (77; 72%). A qualitative research design is used in 63 (59%) literature items of which the majority involve case/interview study research (45, 71%), that is, detailed case studies, briefer case vignettes, or overview studies based on case interviews. Thus, case interviews (56; 52%) and case documents (31; 29%) are the predominant methods used for gathering data across 107 literature items. Different forms of coding are primarily applied as the method for data analysis (30; 28%). Figure 3 provides an overview of the research setup used.
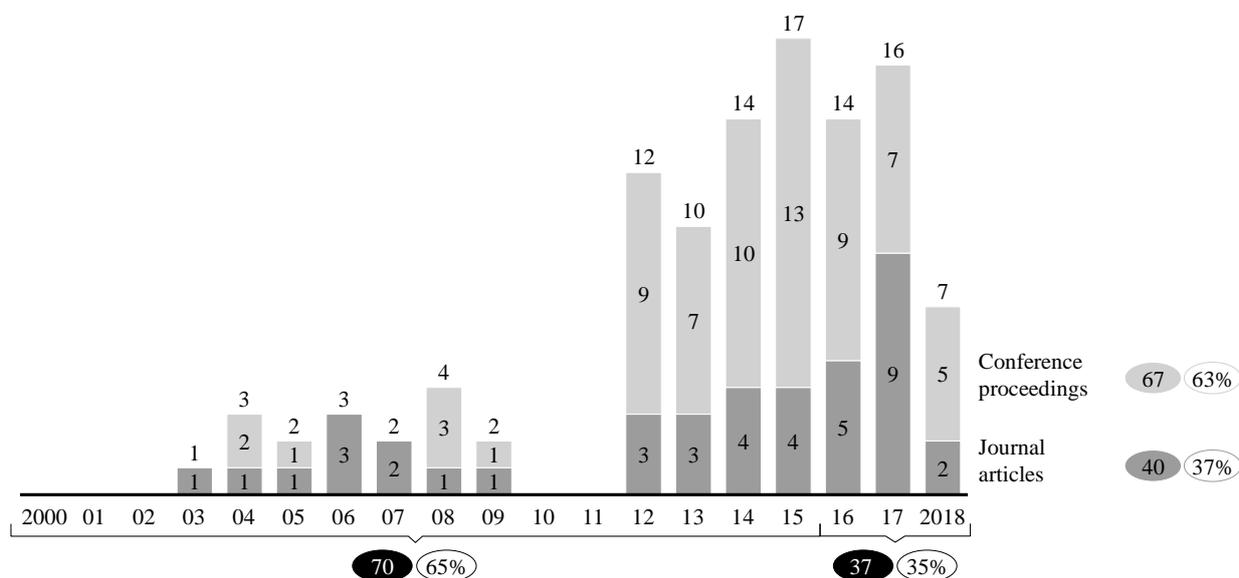

Figure 2. Number of published literature items over time, including relevant literature items from 01/2000 to 08/2018

In our literature review, we identified more than 30 reference theories and subsequent theories to describe and analyze Shadow IT and Business-managed IT, such as transaction cost economics, power relations, actor-network theory, the technology acceptance model, and agency theory. Hence, we draw a similar conclusion as Kopper and Westner [13]: researchers explain Shadow IT and Business-managed IT using a variety of theories, and demonstrate that a dominant approach does not exist.

We analyzed the content of the relevant literature items using open coding [39] with an initial coding scheme based on the research themes identified by Kopper and Westner [13] to ensure research continuity. We structured identified research themes in a framework and iterated the coding and the structuring of the research themes/codes several times (for the detailed coding scheme, please refer to Figure 7 in the appendix). The codes were validated by the second, third, and fourth authors using random sampling. Thus, 14 of the literature items were completely recoded during the coding validation with an exact match for most of the codes (125, 82%). The remaining 27 (18%) codes have been

discussed among the authors, and, as a result, 20 of the original codes (13%) were kept based on an aligned coding scheme, and 7 (5%) of the codes were adjusted. We portray the coding results and the research setup in a concept matrix [33], see Figure 8 in the appendix.

Research design								
Qualitative	63	Quantitative	16	Mixed method	6	Non-empirical	22

Research approach								
Case/interview study	45	Survey research	11	Convent parallel	4	Non-empirical	22
Grounded theory	16	Experimental research	5	Exploratory sequential	2		
Design science	4						
Action design	3						
Ethnography	2						
Unspecific	4						

Worldview		Data gathering		Data analysis	
Constructivist	77	Case interview	56	Coding	30
Post-positivist	19	Case documents	31	Partial least squares	12
Pragmatic	8	Survey	22	Hypothesis test	3
Transformative	3	Non-empirical	22	Context–mechanism–outcome	1
		Observation	19	Network analysis	1
		Expert interview	11	(Logistic) regression	1
		(Laboratory) experiment	5	Average marginal effects	1
		Unspecific	4	Analysis of variance	1
				Risk map	1
				Unspecific	36
				Non-empirical	22

Figure 3. Research setup with absolute frequency of usage (Numbers may not add up to the total of 107 literature items due to the potential use of multiple research, data gathering, and data analysis approaches in literature items, based on Creswell [36])

4. Results

4.1 Categorization framework

We structure the research themes in a framework with three categories: causing factors, outcomes, and governance. Even though we use the framework of Kopper and Westner [13] as an initial coding scheme, we apply more neutral terminology for the categories in comparison to Kopper and Westner [13] since we cover both Shadow IT and Business-managed IT in this literature review. Thus, we refer to causing factors instead of causes and outcomes instead of consequences. Figure 4 shows the resulting framework of causing factors, outcomes, and governance with subcategories and research themes for the three categories. It also includes the relative representation of the research themes in the analyzed body of research covering the concepts of Shadow IT and Business-managed IT.

4.2 Causing factors

We distinguish three subcategories of causing factors: *Enablers (E), Motivators (M),* and *Missing barriers (MB).*

E1 Technical accessibility. This occurs when the accessibility of the IT increases through a general decrease in the complexity of IT and an expansion of technological offerings [40]. As IT solutions become more user-friendly [2], it also becomes easier for BUs to deploy them autonomously [23, 41, 42]. Web services and solutions play a significant role in this evolution [43]. This also applies to cloud offerings with simpler application distribution models [9]. In addition, platforms for end-user development, such as low-code platforms, make it easier for business units to implement their solutions [18, 44, 45]. End-user hardware, such as smartphones [41], and IT consumerization [46] make it easier to access applications and solutions [47–49].

E2 IT user competence. The availability of IT knowledge increases in BUs [10, 42]. This enables BUs to employ or procure IT solutions [50]. In particular, digital natives, who grew up with IT and use it in their daily life, can easily create and access IT solutions [48, 51, 52].

M1 IT organization and BU non-alignment. A lack of business knowledge in the IT organization [53, 54] together with a lack of understanding due to insufficient communication [55] leads to unmet user needs [56–58]. Likewise, users are not sufficiently trained, for example, in operating the central system [59], and business processes are not sufficiently supported [22, 60, 61], for example, due to a high degree of process formalization with extensive documentation requirements even for small pilot projects [62, 63]. Consequently, BUs make detrimental experiences with the IT organization over time [61, 64], which leads to a low level of trust between BUs and the IT organization [41, 65, 66]. In conclusion, this lack of business-IT alignment motivates Shadow IT and Business-managed IT [67–69].

M2 IT system shortcomings. The limitations of existing systems might be overcome by Shadow IT or Business-managed IT [6, 70, 71]; therefore, inadequate IT solutions lead to the deployment of Shadow IT and Business-managed IT [72]. For example, formal IT systems might be perceived as complex and inflexible [21, 72, 73] and hence, insufficient [51, 74, 75] for processes such as enabling communication between employees [76]. Thus, a gap between the users' requirements and the provided systems exists [42, 61, 64], which can be termed an IT systems gap. Furthermore, malfunctioning IT solutions are in place [77, 78], which, for example, hold incorrect data [79–81]. As a particular example, shortcomings of the corporate ERP system are mentioned in multiple literature items [43, 82, 83].

M3 Employee motivation/impact orientation & peer behavior. Shadow IT users have a higher motivation and goal-orientation in comparison to co-workers not using Shadow IT [63, 74, 84]. Thus, the anticipation of increased individual task performance [85], job performance [76, 86, 87], or the prospect of reward [88] leads to Shadow IT and Business-managed IT. Employees even accept potential risks when employing IT autonomously [22, 89]. Moreover, peer behavior influences the use of Shadow IT [90–92]. Employees also might want to conceal their personal misconduct, for example, when a project was not finished in the given timeframe and thus continues as an Un-enacted Project [62].

M4 IT organization slowness. Slow responsiveness to requests [43, 57, 93] is a symptom of IT organizations' lack of agility [55, 58, 94]. A common contribution factor is a disadvantageous prioritization mechanism for requests [50, 95], resulting in long development times [12, 64, 67] and lengthy procurement processes [49]. This lack in the agility of the IT organization fosters the emergence of Shadow IT and Business-managed IT.

M5 Beneficial cost structure anticipation. Shadow IT and Business-managed IT are expected to have lower costs than solutions that are developed by the IT organization [60, 67, 71]. For example, low initial costs [12, 50, 60] are a typical result of renting technology rather than buying it upfront [96].

M6 Business environment uncertainty. Uncertain conditions increase the likelihood of Shadow IT development and implementation, including the need to react to volatile market conditions with high flexibility [6]. Uncertainty in the business environment can be caused by increased competition [67], the need to diversify the product portfolio [53, 54], or strategic needs [62, 63].

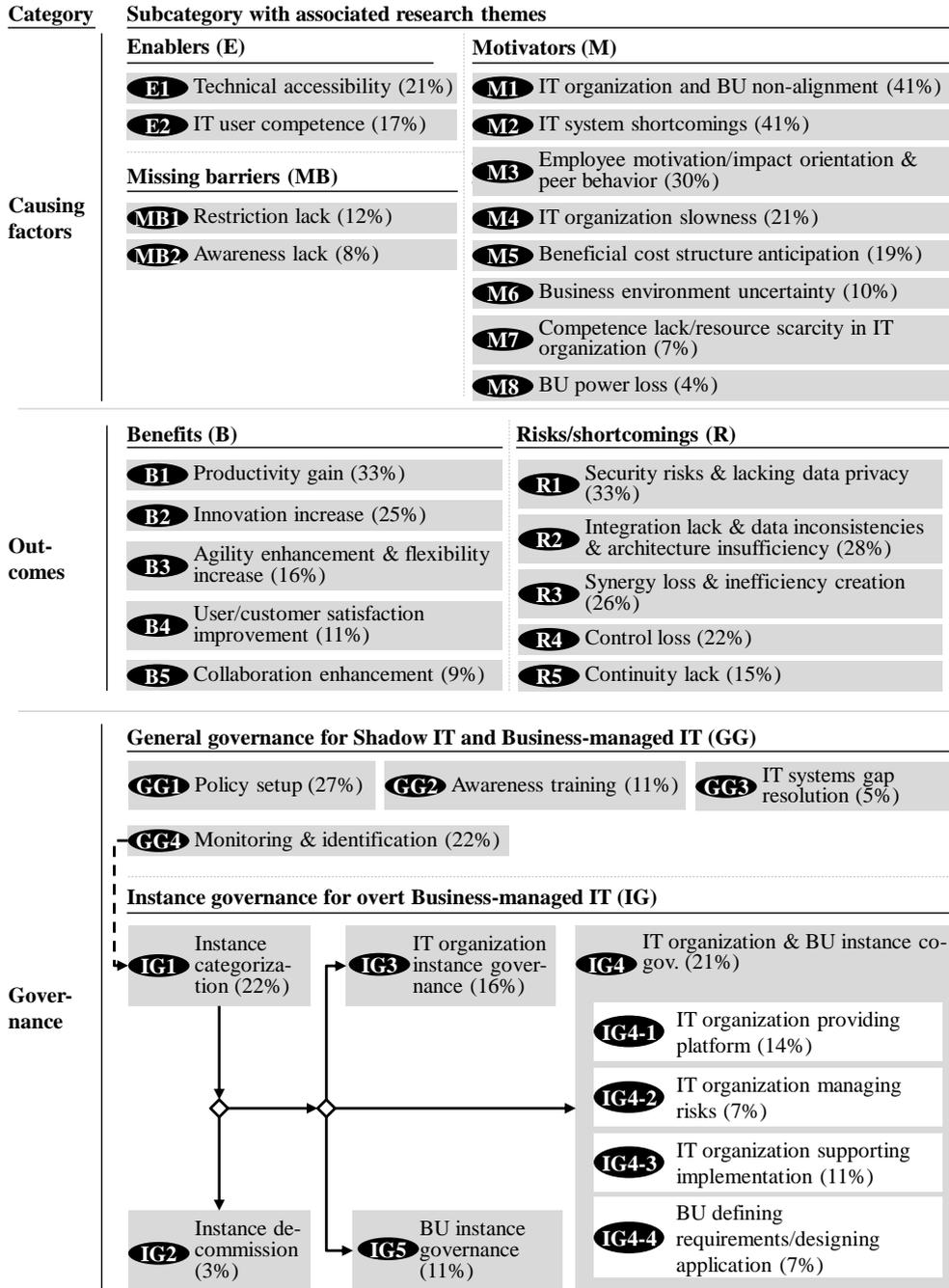(#%) Relative representation of research theme in literature items

Category	Subcategory with associated research themes	
	Enablers (E)	**Motivators (M)**
	E1 Technical accessibility (21%)	**M1** IT organization and BU non-alignment (41%)
	E2 IT user competence (17%)	**M2** IT system shortcomings (41%)
Causing factors	**Missing barriers (MB)**	**M3** Employee motivation/impact orientation & peer behavior (30%)
	MB1 Restriction lack (12%)	**M4** IT organization slowness (21%)
	MB2 Awareness lack (8%)	**M5** Beneficial cost structure anticipation (19%)
		M6 Business environment uncertainty (10%)
		M7 Competence lack/resource scarcity in IT organization (7%)
		M8 BU power loss (4%)
	Benefits (B)	**Risks/shortcomings (R)**
	B1 Productivity gain (33%)	**R1** Security risks & lacking data privacy (33%)
	B2 Innovation increase (25%)	**R2** Integration lack & data inconsistencies & architecture insufficiency (28%)
Out-comes	**B3** Agility enhancement & flexibility increase (16%)	**R3** Synergy loss & inefficiency creation (26%)
	B4 User/customer satisfaction improvement (11%)	**R4** Control loss (22%)
	B5 Collaboration enhancement (9%)	**R5** Continuity lack (15%)

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

GG1 Policy setup (27%)   **GG2** Awareness training (11%)   **GG3** IT systems gap resolution (5%)

GG4 Monitoring & identification (22%)

Instance governance for overt Business-managed IT (IG)

IG1 Instance categorization (22%)

IG3 IT organization instance governance (16%)

IG4 IT organization & BU instance co-gov. (21%)

IG4-1 IT organization providing platform (14%)

IG4-2 IT organization managing risks (7%)

IG4-3 IT organization supporting implementation (11%)

IG2 Instance de-commission (3%)

IG5 BU instance governance (11%)

IG4-4 BU defining requirements/designing application (7%)

Figure 4. Framework for causing factors, outcomes, and governance of Shadow IT and Business-managed IT

M7 Competence lack/resource scarcity in IT organization. A less common motivator for Shadow IT and Business-managed IT comprises a lack of specific IT know-how [64, 71] or missing resources in the IT organization [1, 71]. For example, Ferneley [2] finds that "there was so much to implement and limited resources" in a case study [2, p. 66] which led to Shadow IT.

M8 BU power loss. Another less common theme is the loss of power of BUs [53, 54]. For example, the implementation of an ERP system can lead to a loss of control over business processes [68, 93]. Hence, the development of Shadow IT can provide employees with an opportunity to "gain back some control" [68, p. 149].

MB1 Restriction lack. Silic and Back [41] find that "[o]ut of nine organi[z]ations, four said that they do not have any IT policy that would encompass Shadow IT" (p. 279). On the one hand, non-existent or insufficient policies [53, 94, 97] are missing barriers to Shadow IT and Business-managed IT. However, prohibitions might have limited effects [98]. On the other hand, few companies officially support Shadow IT [41, 56].

MB2 Awareness lack. Employees are typically not aware of the policies in place. For example, Dittes et al. [99] find that "80% [of employees] who violate IT standards do not know that they violate them" (p. 6). Even if employees are aware that policies are in place, they typically do not know their specific content [75]. Besides, employees are not aware of the potential consequences of Shadow IT [55, 84, 94], for example, with concern to violating a regulation [100].

4.3 Outcomes

We designate *Benefits (B)* and *Risks/shortcomings (R)* as subcategories of the outcomes of Shadow IT and Business-managed IT and explore specific research themes of each.

B1 Productivity gain. Because Shadow IT and Business-managed IT, companies benefit from an increase in productivity [6, 51, 101], efficiency [22, 102, 103], and effectiveness [97]. This is mainly driven by productivity gains among employees [84] as Shadow IT leads to improved individual performance [60, 86, 104]. Thus, workflows are improved , and business processes are better supported [2, 43]. Moreover, McGill [105] supports the notion that users perform better with self-developed solutions over solutions developed by others.

B2 Innovation increase. Shadow IT and Business-managed IT can be a source of creativity [95] and innovation [23, 106, 107] as "a manifestation of users' creativity and personal innovativeness" [84, p. 14]. For example, Zimmermann et al. [6] identified a "web-based platform with highly specific construction drawing, order scheduling, and calculation functionalities to support the order-management process of sales representatives and engineers" (p. 6) that was developed by employees as Shadow IT. This shows that, innovations can materialize in new digital services [58] and the usage of consumer IT [108], digital platforms [44], or via lightweight IT [109].

B3 Agility enhancement & flexibility increase. Agility is another benefit of Shadow IT and Business-managed IT [1, 58, 104]. Generated agility can have multiple angles, e.g., shortened time-to-market or agile processes [58]. Moreover, Shadow IT and Business-managed IT usually provide higher flexibility [17, 77, 95] due to their adaptability [8], especially in comparison to large, rigid solutions such as ERP systems [95].

B4 User/customer satisfaction improvement. Shadow IT and Business-managed IT is popular with employees and can lead to higher user satisfaction [57] as it can provide specific functionality [95] or familiarity [51]. Besides, users attribute a higher quality to self-developed applications [83, 105], which leads to better decision performance [105]. If Shadow IT and Business-managed IT is customer-facing, it can also improve customer satisfaction [2, 61, 66].

B5 Collaboration enhancement. Certain Shadow IT and Business-managed IT instances enable better and faster communication [23, 41, 102], such as in the case of knowledge sharing [103]. Hence, the social presence of employees increases [90] and collaboration is fostered [95]. During the creation of Shadow IT and Business-managed IT, enhanced communication can also be observed [84].

R1 Security risks & lacking data privacy. Security risks are commonly associated with Shadow IT [71, 103, 110]; for example, 88% of interviewees mentioned security risks as a downside of Shadow IT [67]. Moreover, in Khalil et al.

[58] each of the ten interviewed IT managers shared security threats, but only four out of the ten interviewed business managers were concerned about security issues. Due to the covert organizational IT management of Shadow IT, typical risk assessment and prevention measures cannot be performed [6], which may lead to compliance issues [49, 60, 64]. Additionally, data privacy cannot be guaranteed [21, 22, 111], particularly for software as a service (SaaS) or for cloud applications [55, 100]. Consequently, Shadow IT poses regulatory risks for enterprises [19, 49, 100] and has the potential for fraud [112].

R2 Integration lack & data inconsistencies & architecture insufficiency. Shadow IT often lacks integration with the official systems [67, 111, 113], is not standardized [16, 54, 60], and might be based on poor architectural principles [53, 54, 98]. Moreover, Shadow IT solutions can lead to data inconsistencies [23, 54, 77] or errors [114, 115]. This results in Myers et al. [115] showing a loss of credibility of data compiled from Shadow IT in their experiments.

R3 Synergy loss & inefficiency creation. The diversification of the IT landscape increases [17, 53, 54] with a simultaneous decrease of standardization [1]. Consequently, synergies cannot be realized [19, 60, 116], redundancies exist [23, 50, 117], and automation is hindered [17, 54]. In summary, inefficiencies occur due to Shadow IT use [1, 64] that lead to higher costs [6, 16, 66], resource waste [57, 93], or resource conflicts with official systems and projects [62, 63, 118].

R4 Control loss. Due to the covert organizational IT management of Shadow IT, gaps in transparency develop [6, 100]; thus, Shadow IT cannot be formally controlled [1, 20, 61]. Hence, Shadow IT undermines IT governance [58], management intentions [22], and strategic goals [12, 40]. It also leads to shifting power relations [54, 58, 80]. Central operations might depend on Shadow IT instances [98], that may result in critical, organizational failrures [53]. In addition, uncontrolled vendor dependencies can exist [58, 71, 97].

R5 Continuity lack. An instance of Shadow IT is often implemented by one or a few employee(s), which leads to a high dependence on such employee(s) for continued operation [53, 95, 105]. Reinforced by lacking documentation [54, 98] and potentially low or non-existing support [43, 60, 103], a risk of system outages exists, leading to operation downtimes [58].

Other outcomes. We summarized three small themes for outcomes below, namely, anticipated economic benefits as well as increased company politics, and IT transformation issues as risks/shortcomings. Anticipated economic benefits have only been realized in a few cases, for example, in the form of reduced transportation costs [61] or via process automation [66]. Shadow IT imposes the risk of spurring political conflicts in companies [95] or even culture wars, perhaps, due to the stigma associated with Shadow IT [43, 69, 95]. Contextual changes, such as the restructuring of the organization or an IT transformation, might significantly impact or be impacted by Shadow IT [71]. One of the reasons for this is that interfaces usually change in an IT transformation and systems need to be updated accordingly [57].

4.4 Governance

Identified Shadow IT instances are overt and are thus Business-managed IT instances. Overt Business-managed IT instances allow for more specific measures as compared to unknown (covert) Shadow IT. After the categorization of Business-managed IT instances, two potential decision points exist: First, a decision for instance decommission or instance continuation can be made. Second, if Business-managed IT instances are continued, governance responsibility can be allocated on a spectrum between complete governance allocation to the IT organization and complete governance allocation to the BU. An intermediary solution on this spectrum would be co-governance between the IT organization and BUs. Below, we first detail the *General governance for Shadow IT and Business-managed IT (GG)* and continue with *Instance governance for overt Business-managed IT (IG)*.

GG1 Policy setup. Considering the benefits of Shadow IT and Business-managed IT, a complete prohibition does not seem to be reasonable [6, 18, 119]. Such a measure would also negatively impact employee motivation [84] and innovation behavior [108]. Hence, it appears to be more promising to allow for Shadow IT and Business-managed IT in a controlled manner [60, 71, 95]. In fact, Ortbach et al. [120] state that trust, which is the underlying principle of a bring

your own device (BYOD) culture, might outweigh the need for stricter policies. However, for critical processes or highly regulated businesses, it may be more reasonable for Shadow IT to be strictly forbidden [12, 50, 60].

GG2 Awareness training. Communication of existing policies, which restrict Shadow IT [66, 67, 84] and aim to minimize potential threats of unapproved IT [87, 97], can increase awareness of the risks of Shadow IT and Business-managed IT. For example, training courses on existing policies can be held [41, 98, 100]. However, increased awareness of risks associated with Shadow IT might not lead to its reduction [58].

GG3 IT systems gap resolution. Shadow IT and Business-managed IT use can be reduced if existing shortcomings of the IT systems are addressed to fulfill unmet needs [40, 56, 97]. However, Haag et al. [84] find that "adapting, fine-tuning, and tailoring the mandatory system will probably not succeed if the aim is to prevent individuals from the usage of shadow systems" (p. 14) as "[t]here was no difference in the perceived usefulness of the mandatory system between those participants that used the shadow system/s and those that did not" (p. 14).

GG4 Monitoring & identification. Technical monitoring can be a measure to enforce policies on Shadow IT [41, 49, 121], but these may also be bypassed by employees [41]. Monitoring helps to identify covert Shadow IT instances, which would then become overt and thus Business-managed IT [1]. Other possibilities to identify Shadow IT include IT architecture assessments [71], the evaluation of help desk requests [52], employee surveys [52, 56], and scanning of installed software on end-user devices [41]. Support for Shadow IT might lead to employees actively engaging with the IT organization for assistance, which would also increase transparency [18, 100].

IG1 Instance categorization. Overt Business-managed IT instances can be categorized, for example, by type of IT/solution [92, 98, 104], creator of solution [103], type of project [62, 63], intention [121], or process/technology and time dimensions [20]. Nevertheless, a categorization by criticality and quality of instances [45, 122, 123], by functional scope and scope of use [17, 71, 122], or by strategic importance and stakeholder [96], is required to define a suitable governance approach.

IG2 Instance decommission. After instance categorization, a primary decision point with two potential outcomes exists: instance decommission or instance continuation. If Business-managed IT has a high architectural inflexibility, [71] or the associated risks are too high [54, 67], instances of Business-managed IT might be decommissioned and potentially replaced by other solutions [67].

IG3 IT organization instance governance. If the continuation of Business-managed IT instances was chosen at the primary decision point a secondary decision point arises to allocate the instance governance. Three potential governance allocations exist on a spectrum of governance responsibility being allocated to the IT organization (IG3) or the BU (IG5). The first potential governance allocation is governance transfer to the IT organization [6, 8, 95], such as for instances with high criticality [8, 54, 98], crucial security concerns [50], or for instances, for which the company-wide view is in favor of the integration with the IT organization [124], or when maintenance is too burdensome for the BU [57].

IG4 IT organization & BU instance co-governance. The second potential governance allocation is co-governance, that is, Business-managed IT instances can be split into service components or into tasks. Moving forward, an allocation of task responsibilities to the IT organization or the BU would be possible [125]. In the following passages, we detail the potential task allocation to the stakeholders.

IG4-1 IT organization providing platform. The IT organization may provide platforms for application development [46, 71]. Those platforms can include the infrastructure layer [1, 12, 109], the data layer [67, 119, 125], or even the application layer [67]. Enterprise app stores can provide a platform for mobile devices [55].

IG4-2 IT organization managing risks. Risk management of instances is usually considered to be ensured by the IT organization [1, 67]. For example, when BUs autonomously develop mobile apps, IT organizations can take over the security and privacy checks [66], or the IT organization ensures security arrangements in a BYOD environment [60] to ensure compliance with company security standards.

IG4-3 IT organization supporting implementation. The IT organization may provide continuous support for the development and implementation of projects conducted in BUs [6, 12, 21] and provide expertise in areas such as project management [67], vendor management [67], service management [1, 119, 125], and collaboration and knowledge exchange [83, 126].

IG4-4 BU defining requirements/designing application. The BUs perform IT-related tasks that require specific business knowledge [1, 119, 125]. Typical tasks include the definition of requirements [1, 119, 125] or the design and development of applications [50, 66, 96].

IG5 BU instance governance. The third potential governance allocation is that BUs govern Business-managed IT entirely [8, 60, 96], such as for instances with limited scope [6, 11] or when business-specific skills are needed for governing and running the Business-managed IT instance [1].

4.5 Longitudinal Analysis

We divided the analyzed time horizon January 2000–June 2018 at the transition point of December 2015–January 2016 to highlight how the research themes evolved, especially as reflected in the older 65% of literature items in comparison to the more recent 35% of items. Moreover, this breakdown illustrates the evolution of themes since the literature review by Kopper and Westner [13], which covers literature items until the end of 2015.

Figure 5 shows the evolution of the coverage of research themes over time.
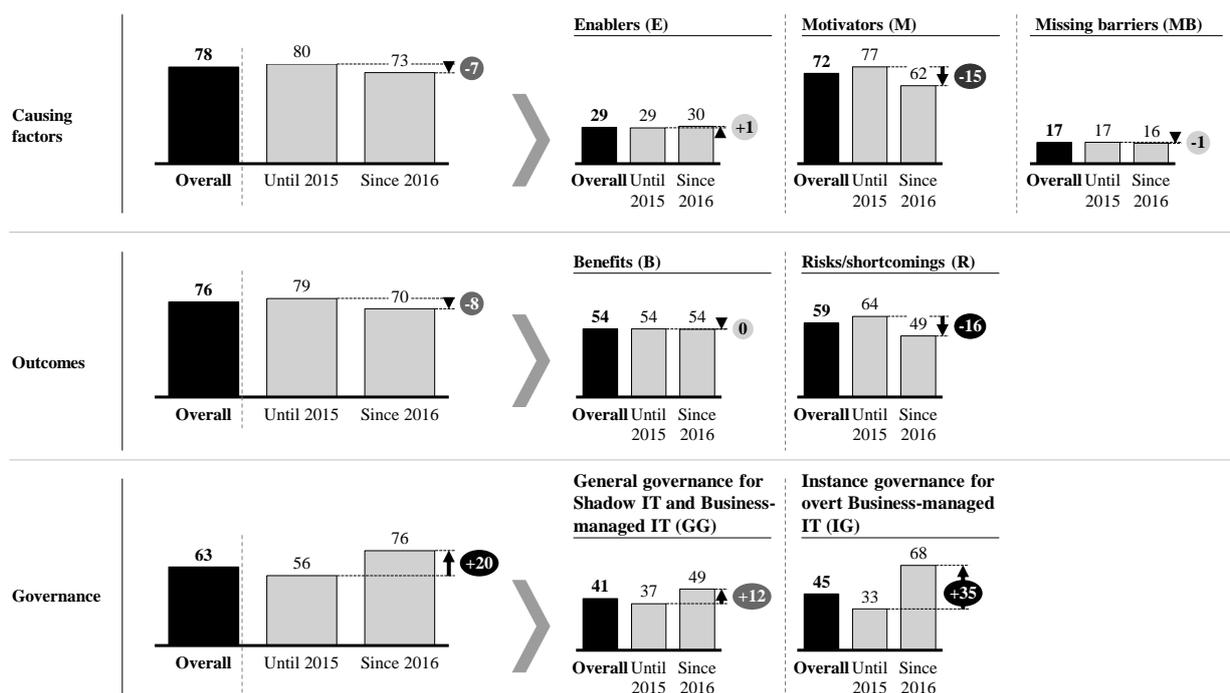

Figure 5. Longitudinal analysis of research attention, percentage of the literature identified mentioning themes in category and subcategory (70 literature items until 2015; 37 items since 2016)

The figure emphasizes that the attention of researchers (based on frequency of mentioned research themes according to the framework in Figure 4) shifted in recent years: recent literature items (since 2016) cover themes with a major focus on governance (76%), whereas causing factors were predominantly (80%) covered in older literature items (until 2015). Hence, themes on governance gained a significant increase in interest in the recent literature.

Besides, Figure 5 exhibits the evolution of themes on a smaller scale through the subcategories. The main subcategories examined in recent literature are: themes about *Instance governance for overt Business-managed IT (IG),* which are covered in 68% of recent literature as compared to 33% of the older literature. Themes about *Motivators (M)* are analyzed in 62% of recent publications. Themes about *Benefits (B)* have 54% coverage. *Risks/shortcomings (R)* and *General governance for Shadow IT and Business-managed IT (GG)* are both examined in 49% of publications. Research themes on *Enablers (E)* and *Missing barriers (MB)*—both subcategories of causing factors—are more specific and are covered in a lower proportion of the literature items.

The detailed evolution of the individual research themes over time is shown in Figure 9 in the appendix. On average, an increase of research coverage across research themes is notable for recent literature items (those published from 2016 onward) as compared to older literature (until 2015). Thus, researchers are, in general, more broadly covering the field of Shadow IT and Business-managed IT. However, several themes gained significant coverage in the literature (15% coverage in recent literature as compared to older literature), namely: *M6 Business environment uncertainty, R4 Control loss, IG1 Instance categorization, IG4-1 IT organization providing platform*, and *IG4-3 IT organization supporting implementation*. Hence, researchers have increasingly published research on the co-governance of Business-managed IT instances and the role of the IT organization in such co-governance settings.

5. Discussion

This paper creates transparency on research themes concerning Shadow IT and Business-managed IT with a deeper analysis of recent literature (since 2016), which comprises 35% of the body of research. As the field has evolved significantly—more than twice as many literature items could be identified compared to the review of Kopper and Westner [13]—research themes are broken down to a more specific level. We identified 34 research themes as compared to 22 themes in Kopper and Westner [13]. Specifically, we could characterize several additional motivators, such as *M1 IT organization and BU non-alignment.* In the outcome category, our results are more detailed for both benefits and risks/shortcomings. For example, we additionally include the themes *B3 Agility enhancement & flexibility increase* and *R5 Continuity lack.* In the governance category, we detail two decision points, namely, (a) instance decommission or continuation and (b) governance allocation, such as in the case of *IG4 IT organization & BU instance co-governance.*

The identified research themes for causing factors consider both Shadow IT and Business-managed IT as Shadow IT instances might become overt during their lifecycle and thus become Business-managed IT. Due to the overt organizational IT management of Business-managed IT, risks/shortcomings are more transparent, and some of these can, therefore, be better mitigated in comparison to Shadow IT [1]. In contrast, benefits can be realized for both Shadow IT and Business-managed IT, independent of their involvement in the organizational IT management (covert/overt). Moreover, Khalil et al. [58] noticed a different perception between business managers 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)" [58, p. 8]. In contrast to this, "IT managers put more emphasis on the threats related to cloud computing (total freq. of 25) than the business manager (total freq. of 6)" [58, p. 9].

When Shadow IT instances are not known ("in the shadows" [1]) only a few governance measures can be applied, that is, the research themes in the category *General governance for Shadow IT and Business managed IT (GG),* including *GG4 Monitoring & identification.* Monitoring & identification can lead to Shadow IT instances becoming overt and thus becoming Business-managed IT instances as they are "not 'in the shadows' anymore" [1, p. 2]. If specific Business-managed IT instances are transparent, they can be categorized. A primary decision point for instance decommission or continuation exists. In the case of the decision for continuation, governance responsibility for

instances can be allocated based on a secondary decision point with three decision outcomes: Governance transferred to the IT organization (i.e., *IG3 IT organization instance governance)*, governance shared between the IT organization and the BU (i.e., *IG4 IT organization & BU instance co-governance)*, or governance kept at BU (i.e., *IG5 BU instance governance)*. The increased detail of Shadow IT and Business-managed IT governance in the scientific literature is also in line with the evolution of research themes over time. For example, the theme *IG4 IT organization & BU co-governance* for Business-managed IT instances has gained significant research attention since 2016. In addition, the longitudinal analysis shows a shift of research attention towards governance themes and away from motivators. This follows a somewhat expected pattern as the older literature (until 2015) sheds light on the motivators for Shadow IT and Business-managed IT in order to understand why these instances occur. As there is a better understanding of causing factors, recent research (since 2016) defines approaches to govern Shadow IT and Business-managed IT in general, as well as instance governance for overt Business-managed IT. Additionally, the recent literature covers a broader range of research themes as compared to literature published until 2015. Hence, future research needs be conducted enhance specific research themes.

Consequently, we argue for three governance recommendations, see Figure 6. First, the existing gaps in IT systems can be addressed. Typically, a gap between users' requirements and the existing systems/hardware/services exists. If this IT systems gap is reduced, a major motivator for Shadow IT and Business-managed IT can be resolved.
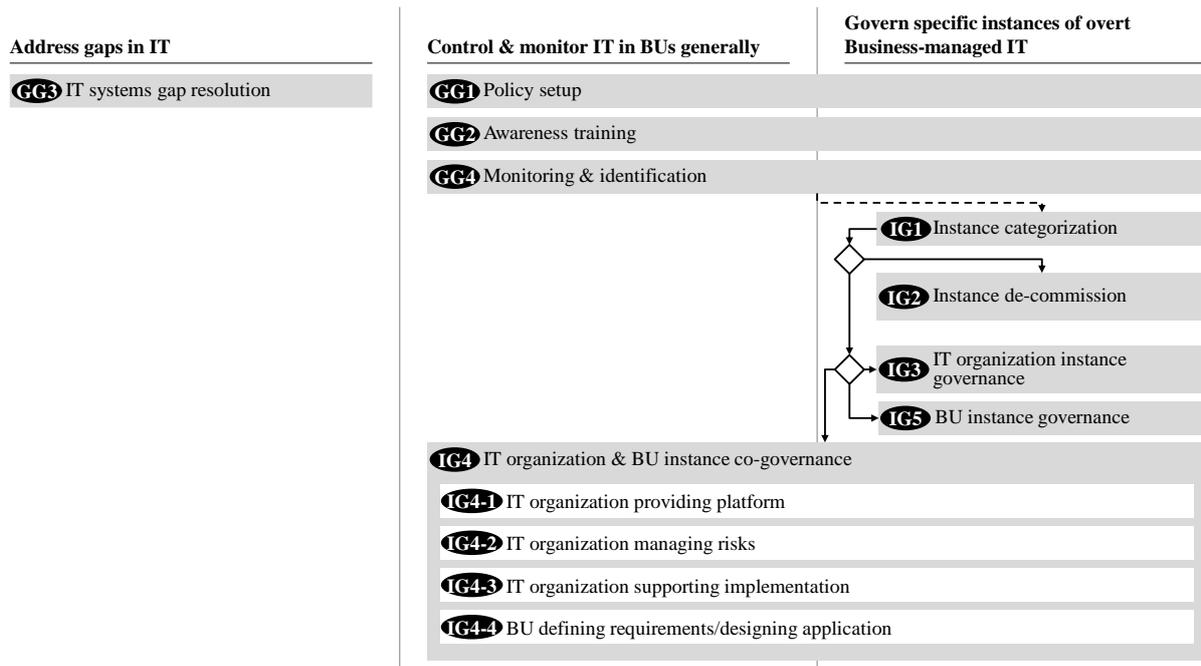

Figure 6. Governance recommendations based on literature review

Second, IT in BUs, that is, Shadow IT and Business-managed IT, can be controlled and monitored on a general level. Policies are governance measures to regulate the use of Shadow IT and Business-managed IT. Awareness creation for Shadow IT and Business-managed IT, as well as the existing policies, make these policies executable. Applications and user behavior can generally be monitored to identify Shadow IT and maintain the transparency of Business-managed IT

instances. Moreover, co-governance approaches can be implemented between the IT organization and the BUs to provide a general environment for IT in BUs, which in turn is based on existing policies.

Third, governance recommendations for specific, existing Business-managed IT instances can be implemented. Depending on the current governance status of specific instances, the previously described governance process can be used. That is, overt instances (e.g., Shadow IT instances that became overt instances after their identification) can be categorized, and thereafter, the governance can be defined via the two decision points: (1) continuation/decommission, (2) allocation of governance of specific instances to the IT organization, the BU, or in a co-governance model. Figure 6 illustrates the described approaches. However, a categorization and explicit governance allocation for specific instances is not possible for covert Shadow IT instances which limits governance measures for Shadow IT. Hence, for Business-managed IT, a broader range of governance measures exists.

6. Conclusion and outlook

In this systematic literature review, we provide a framework for Shadow IT and Business-managed IT assessing research themes within three categories: Causing factors, outcomes, and governance. For causing factors, we identify the subcategories enablers, motivators, and missing barriers. For outcomes, we find benefits and risks/shortcomings in the literature. As subcategories for governance, we identify general governance for Shadow IT and Business-managed IT and instance governance for overt Business-managed IT. The differences in the body of research until 2015 and since 2016 show that governance themes are gaining attention among researchers; in contrast, the older literature focused on motivators for Shadow IT and Business-managed IT. This is in line with the progress of the research field.

Moreover, we build on the recently introduced framework of Kopper et al. [1]. We differentiate Shadow IT (covert instances) and Business-managed IT (overt instances) and provide an allocation of relevant research themes for the two concepts. Shadow IT and Business-managed IT may share the same causing factors since different trajectories for instances exist. For example, instances can start as covert Shadow IT and become overt Business-managed IT due to monitoring mechanisms and subsequent identification. However, Business-managed IT promises to avoid some of the risks/ shortcomings of Shadow IT due to its involvement in the organizational IT management, while providing similar benefits [1]. Particularly, additional governance measures exist if Business-managed IT instances are overt, as compared to covert Shadow IT instances.

Practitioners can build on the framework of causing factors, outcomes, and governance to evaluate instances of Shadow IT and Business-managed IT. In general, organizations should take advantage of the benefits of Shadow IT and Business-managed IT, but also need to address the risks/shortcomings of Shadow IT in such instances. The provided governance recommendations can be used by practitioners as references to allocate governance responsibilities on a general level and for existing instances.

The paper helps to structure areas for further research on Shadow IT and Business-managed IT. First, further research could embed the two concepts of Shadow IT and Business-managed IT in related IS research streams. Related research streams include, (a) agile/embedded IT, (b) outsourcing (as Business-managed IT could also be understood as IT outsourcing from the perspective of the IT organization), or (c) central/decentral IT among others. Hence, an overarching taxonomy of related research streams would be beneficial to illustrate the commonalities and differences and to provide a basis for leveraging research findings across the streams. Second, further differentiation of the two concepts, Shadow IT and Business-managed IT, would be beneficial for the field. For example, researchers can shed light on the trajectory of instances of Shadow IT and Business-managed IT. Moreover, researchers could study the practitioner perceptions of both concepts. Third, as Business-managed IT was very recently introduced as a concept, further research could advance the concept and its facets. Due to the development of the research field and the broad focus of the existing literature, focused research on specific themes would advance the field considerably. Future research should target outcomes and governance themes because causing factors have been widely studied in existing research. Consequently, an evaluation of the business value of Shadow IT or Business-managed IT that considers the benefits and risks/shortcomings is a fourth area for future research. Accordingly, the business value might be different

for the BU (on a local level) as compared to the whole organization (on a general level). Fifth, the existing governance approaches as well as further governance approaches should be discussed, particularly as low-code platforms become a basis for Business-managed IT.

References

[1] A. Kopper *et al.,* "Business-managed IT: A Conceptual Framework and Empirical Illustration," in *Proceedings of the 26th European Conference on Information Systems*, Portsmouth, UK, 2018.

[2] E. H. Ferneley, "Covert End User Development: A Study of Success," *Journal of Organizational and End User Computing*, vol. 19, no. 1, pp. 62–71, 2007.

[3] A. Kopper *et al.,* "Shadow IT and Business-Managed IT: A Conceptual Framework and Empirical Illustration," *International Journal of IT/Business Alignment and Governance*, vol. 9, no. 2, pp. 53–71, 2018.

[4] M. Segal, *Dealing with the Realities of Shadow IT.* [Online] Available: http://www.datacenterjournal.com/dealing-realities-shadow. Accessed on: May 11 2018.

[5] K. Corbin, *Cios Vastly Underestimate Extent of Shadow IT.* [Online] Available: https://www.cio.com/article/2968281/cio-role/cios-vastly-underestimate-extent-of-shadow-it.html. Accessed on: May 11 2018.

[6] S. Zimmermann, C. Rentrop, and C. Felden, "A Multiple Case Study on the Nature and Management of Shadow Information Technology," *Journal of Information Systems*, vol. 31, no. 1, pp. 79–101, 2017.

[7] A. Kopper and M. Westner, "Towards a Taxonomy for Shadow IT," in *Proceedings of the 22nd Americas Conference on Information Systems*, San Diego, USA, 2016, pp. 1–10.

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

[9] S. Haag and A. Eckhardt, "Shadow IT," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 469–473, 2017.

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

[11] T. J. Winkler and C. V. Brown, "Horizontal Allocation of Decision Rights for On-Premise Applications and Software-as-a-Service," *Journal of Management Information Systems*, vol. 30, no. 3, pp. 13–48, 2013.

[12] C. E. H. Chua and V. C. Storey, "Bottom-Up Enterprise Information Systems," *Communications of the Association for Information Systems*, vol. 60, no. 1, pp. 66–72, 2016.

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

[14] J. Magunduni and W. Chigona, "Revisiting Shadow IT Research: What We Already Know, What We Still Need to Know, and How Do We Get There?," in *Proceedings of the Conference on Information Communications Technology and Society*, Durban, South Africa, 2018, pp. 1–6.

[15] S. Alter, "Theory of Workarounds," *Communications of the Association for Information Systems*, vol. 34, no. 1, pp. 1041–1066, 2014.

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

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

[18] A. Kopper, M. Westner, and S. Strahringer, "Kontrollierte Nutzung von Schatten-IT," *HMD Praxis der Wirtschaftsinformatik*, vol. 54, no. 1, pp. 97–110, 2017.

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

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

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

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

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

[24] Y. Levy and T. J. Ellis, "A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research," *Informing Science: The International Journal of an Emerging Transdiscipline*, vol. 9, pp. 181–212, 2006.

[25] C. Okoli, "A Guide to Conducting a Standalone Systematic Literature Review," *Communications of the Association for Information Systems*, vol. 37, pp. 879–910, 2015.

[26] J. vom Brocke *et al.,* "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," in *Proceedings of the 17th European Conference on Information Systems*, Verona, Italy, 2009, pp. 1–12.

[27] F. Rowe, "What Literature Review Is Not: Diversity, Boundaries and Recommendations," *European Journal of Information Systems*, vol. 23, no. 3, pp. 241–255, 2014.

[28] W. Bandara, S. Miskon, and E. Fielt, "A Systematic, Tool-Supported Method for Conducting Literature Reviews in Information Systems," in *Proceedings of the 19th European Conference on Information Systems*, Helsinki, Finland, 2011, pp. 1–13.

[29] H. M. Cooper, "Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews," *Knowledge in Society*, vol. 1, no. 1, pp. 104–126, 1988.

[30] H. M. Cooper and L. V. Hedges, "Research Synthesis as a Scientific Process," in *The Handbook of Research Synthesis and Meta-Analysis*, H. M. Cooper, L. V. Hedges, and J. C. Valentine, Eds., 2nd ed., New York: Russell Sage Foundation, 2009, pp. 3–16.

[31] T. P. Herz, F. Hamel, F. Uebernickel, and W. Brenner, "Deriving a Research Agenda for the Management of Multisourcing Relationships Based on a Literature Review," in *Proceedings of the 16th Americas Conference on Information Systems*, Lima, Peru, 2010, pp. 1–11.

[32] A. Strasser and M. Westner, "Information Systems Offshoring: Results of a Systematic Literature Review," *Journal of Information Technology Management*, vol. 26, no. 2, pp. 70–142, 2015.

[33] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a literature Review," *MIS Quarterly*, vol. 26, no. 2, pp. xiii–xxiii, 2002.

[34] C. Okoli and K. Schabram, "A Guide to Conducting a Systematic Literature Review of Information Systems Research," *Sprouts: Working Papers on Information Systems*, vol. 10, no. 26, pp. 1–50, 2010.

[35] G. Paré, M.-C. Trudel, M. Jaana, and S. Kitsiou, "Synthesizing Information Systems Knowledge: A Typology of Literature Reviews," *Information & Management*, vol. 52, no. 2, pp. 183–199, 2015.

[36] J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Los Angeles, London, New Delhi, Singapore, Washington DC: SAGE Publications, 2014.

[37] U. Stödberg, "A Research Review of E-Assessment," *Assessment & Evaluation in Higher Education*, vol. 37, no. 5, pp. 591–604, 2012.

[38] S. Jalali and C. Wohlin, "Global Software Engineering and Agile Practices: A Systematic Review," *Journal of Software: Evolution and Process*, vol. 24, no. 6, pp. 643–659, 2012.

[39] W. L. Neuman, *Social Research Methods: Qualitative and Quantitative Approaches,* 7th ed. Harlow: Pearson Education Limited, 2013.

[40] S. Zimmermann and C. Rentrop, "Schatten-IT," *HMD Praxis der Wirtschaftsinformatik*, vol. 49, no. 6, pp. 60–68, 2012.

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

[42] A. Spierings, D. V. Kerr, and L. Houghton, "Issues that support the creation of ICT workarounds: towards a theoretical understanding of feral information systems," *Information Systems Journal*, vol. 27, no. 6, pp. 775–794, 2017.

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

[44] D. Sedera, S. Lokuge, V. Grover, S. Sarker, and S. Sarker, "Innovating with Enterprise Systems and Digital Platforms: A Contingent Resource-Based Theory View," *Information & Management*, vol. 53, no. 3, pp. 366–379, 2016.

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

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

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

[48] R. M. Davison, C. X.J. Ou, and Y. Chang, "Subverting Organisational IS Policy with Feral Systems: A Case in China," *Industrial Management & Data Systems*, vol. 118, no. 3, pp. 570–588, 2018.

[49] R. Walters, "Bringing IT out of the Shadows," *Network Security*, vol. 2013, no. 4, pp. 5–11, 2013.

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

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

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

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

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

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

[56] M. Walterbusch, A. Fietz, and F. Teuteberg, "Schatten-IT: Implikationen und Handlungsempfehlungen für Mobile Security," *HMD Praxis der Wirtschaftsinformatik*, vol. 51, no. 1, pp. 24–33, 2014.

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

[58] S. Khalil, T. J. Winkler, and X. Xiao, "Two Tales of Technology: Business and IT Managers' Technological Frames Related to Cloud Computing," in *Proceedings of the 38th International Conference on Information Systems*, Seoul, South Korea, 2017, pp. 1–20.

[59] L. Houghton and D. V. Kerr, "Feral Information Systems Creation as Sensemaking," *Systems*, vol. 3, no. 4, pp. 330–347, 2015.

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

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

[62] A. Buchwald and N. Urbach, "Implikationen von inoffiziellen Projekten für die IT-Governance," *HMD Praxis der Wirtschaftsinformatik*, vol. 51, no. 3, pp. 319–329, 2014.

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

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

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

[66] M. Silic, D. Silic, and G. Oblakovic, "Influence of Shadow IT on Innovation in Organizations," *Complex Systems Informatics and Modeling Quarterly*, no. 8, pp. 68–80, 2016.

[67] A. Kopper, "Perceptions of IT Managers on Shadow IT," in *Proceedings of the 23rd Americas Conference on Information Systems*, Boston, USA, 2017, pp. 1–10.

[68] D. V. Kerr, L. Houghton, and K. Burgess, "Power Relationships that Lead to the Development of Feral Systems," *Australasian Journal of Information Systems*, vol. 14, no. 2, pp. 141–152, 2007.

[69] L. Houghton and D. V. Kerr, "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*, vol. 4, no. 2, pp. 135–147, 2006.

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

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

[72] S. Huuskonen and P. Vakkari, ""I Did It My Way": Social Workers as Secondary Designers of a Client Information System," *Information Processing & Management*, vol. 49, no. 1, pp. 380–391, 2013.

[73] M.-C. Boudreau and D. Robey, "Enacting Integrated Information Technology: A Human Agency Perspective," *Organization Science*, vol. 16, no. 1, pp. 3–18, 2005.

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

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

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

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

[78] P. Koopman and R. R. Hoffman, "Work-Arounds, Make-Work, and Kludges," *IEEE Intelligent Systems*, vol. 18, no. 6, pp. 70–75, 2003.

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

[80] B. Azad and N. King, "Institutional Analysis of Persistent Computer Workarounds," in *Proceedings of the Academy of Management*, Chicago, USA, 2009, pp. 1–41.

[81] S. Kent, L. Houghton, and D. V. Kerr, "Affective Events Theory, Institutional Theory and feral Systems: How do they all Fit?," in *Proceedings of the 27th Australian and New Zealand Academy of Management Conference*, Hobart, Australia, 2013.

[82] L. Silva and H. K. Fulk, "From Disruptions to Struggles: Theorizing Power in ERP Implementation Projects," *Information and Organization*, vol. 22, no. 4, pp. 227–251, 2012.

[83] K. Lyytinen and M. Newman, "A Tale of Two Coalitions - Marginalising the Users While Successfully Implementing an Enterprise Resource Planning System," *Information Systems Journal*, vol. 25, no. 2, pp. 71–101, 2015.

[84] S. Haag, A. Eckhardt, and C. Bozoyan, "Are Shadow System Users the Better IS Users? – Insights of a Lab Experiment," in *Proceedings of the 36th International Conference on Information Systems*, Fort Worth, USA, 2015, pp. 1–20.

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

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

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

[88] D. V. Kerr and L. Houghton, "Feral Systems: The Likely Effects on Business Analytics Functions in an Enterprise Resource Planning System Environment," in *Proceedings of the 19th Australasian Conference on Information Systems*, Christchurch, New Zealand, 2008, pp. 484–491.

[89] M. Silic, J. B. Barlow, and A. Back, "A New Perspective on Neutralization and Deterrence: Predicting Shadow IT Usage," *Information & Management*, vol. 54, no. 8, pp. 1023–1037, 2017.

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

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

[92] G. L. Mallmann, A. C. Maçada, and A. Eckhardt, "We are Social: A Social Influence Perspective to Investigate Shadow IT Usage," in *Proceedings of the 26th European Conference on Information Systems*, Portsmouth, UK, 2018, pp. 1–16.

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

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

[95] S. Behrens, "Shadow Systems: The Good, The Bad and The Ugly," *Communications of the Association for Information Systems*, vol. 52, no. 2, pp. 124–129, 2009.

[96] S. J. Andriole, "Who Owns IT?," *Communications of the Association for Information Systems*, vol. 58, no. 3, pp. 50–57, 2015.

[97] M. Walterbusch, A. Fietz, and F. Teuteberg, "Missing Cloud Security Awareness: Investigating Risk Exposure in Shadow IT," *Journal of Enterprise Information Management*, vol. 30, no. 4, pp. 644–665, 2017.

[98] C. Rentrop, S. Zimmermann, and M. Huber, "Schatten-IT – ein unterschätztes Risiko?," in *Proceedings of the D·A·CH Security Conference*, 2015, pp. 291–300.

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

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

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

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

[103] G. L. Mallmann, A. C. Maçada, and M. Oliveira, "The Influence of Shadow IT Usage on Knowledge Sharing: An Exploratory Study with IT Users," *Business Information Review*, vol. 35, no. 1, pp. 17–28, 2018.

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

[105] T. J. McGill, "The Effect of End User Development on End User Success," *Journal of Organizational and End User Computing*, vol. 16, no. 1, pp. 41–58, 2004.

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

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

[108] S. Köffer, K. Ortbach, I. Junglas, B. Niehaves, and J. Harris, "Innovation Through BYOD?: The Influence of IT Consumerization on Individual IT Innovation Behavior," *Business & Information Systems Engineering*, vol. 57, no. 6, pp. 363–375, 2015.

[109] B. Bygstad, "Generative Innovation: A Comparison of Lightweight and Heavyweight IT," *Journal of Information Technology*, vol. 32, no. 2, pp. 180–193, 2017.

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

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

[112] A. Shaikh, "Shadow-IT System and Insider Threat: An Assessment of an Opportunity Dimension for the Identity Theft," in *20th HCI International Conference*, Las Vegas, USA, 2018, pp. 314–317.

[113] B. Azad and N. King, "Institutionalized Computer Workaround Practices in a Mediterranean Country: An Examination of Two Organizations," *European Journal of Information Systems*, vol. 21, no. 4, pp. 358–372, 2012.

[114] R. R. Panko, "Spreadsheets and Sarbanes-Oxley: Regulations, Risks, and Control Frameworks," *Communications of the Association for Information Systems*, vol. 17, pp. 1–29, 2006.

[115] N. Myers, M. W. Starliper, S. L. Summers, and D. A. Wood, "The Impact of Shadow IT Systems on Perceived Information Credibility and Managerial Decision Making," *Accounting Horizons*, vol. 31, no. 3, pp. 105–123, 2017.

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

[117] J. Peppard, "The Application of the Viable Systems Model to Information Technology Governance," in *Proceedings of the 26th International Conference on Information Systems*, Las Vegas, USA, 2005, pp. 45–58.

[118] B. S. Blichfeldt and P. Eskerod, "Project Portfolio Management: There's More to IT Than What Management Enacts," *International Journal of Project Management*, vol. 26, no. 4, pp. 357–365, 2008.

[119] S. Zimmermann, C. Rentrop, and C. Felden, "Governing IT Activities in Business Workgroups—Design Principles for a Method to Control Identified Shadow IT," in *Proceedings of the 19th International Conference on Business Information Systems*, Leipzig, Germany, 2016, pp. 252–264.

[120] K. Ortbach, T. Brockmann, and S. Stieglitz, "Drivers for the Adoption of Mobile Device Management in Organizations," in *Proceedings of the 22nd European Conference on Information Systems*, Tel Aviv, Isreal, 2014, pp. 1–18.

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

[122] C. Rentrop and S. Zimmermann, "Shadow IT Evaluation Model," in *Proceedings of the Federated Conference on Computer Science and Information Systems*, Wroclaw, Poland, 2012, pp. 1023–1027.

[123] E. H. Ferneley and P. Sobreperez, "Resist, Comply or Workaround? an Examination of Different Facets of User Engagement with Information Systems," *European Journal of Information Systems*, vol. 15, no. 4, pp. 345–356, 2006.

[124] M. Huber, S. Zimmermann, C. Rentrop, and C. Felden, "Toward a Conceptual Decision Framework for Shadow IT Integration," in *Proceedings of the 24th Americas Conference on Information Systems*, New Orleans, USA, 2018, pp. 1–5.

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

[126] J. Peppard, "Rethinking the Concept of the Is Organization," *Information Systems Journal*, vol. 28, no. 1, pp. 76–103, 2016.

Appendix A. Coding scheme

Category	Subcategory	Research theme	Keywords/phrases for coding
Causing factors	**Enablers**	**E1** Technical accessibility	▪ Cloud/web services and solutions/SaaS ▪ IT becoming user friendly/open source ▪ Smartphones, iPads, BYOD ▪ Platforms for end-user development
		E2 IT user competence	▪ IT knowledge in BU ▪ Digital natives, tech savvy users
	Motivators	**M1** IT organization and BU non-alignment	▪ Unsatisfied needs of business/users ▪ Lacking business knowledge in IT ▪ Unsupported business processes ▪ Bad past experiences/low level of trust ▪ Lack of alignment/poor business-IT alignment
		M2 IT system shortcomings	▪ Inadequate IT solutions ▪ IT systems gap ▪ Malfunctioning of existing IT solution ▪ Limitations of IT system/tools ▪ Inflexibility/complexity of IT system ▪ Shortcomings of ERP system
		M3 Employee motivation/ impact orientation & peer behavior	▪ Efficient individual task performance/goal-orientation/high motivation ▪ Experienced individual frustration ▪ Peer behavior
		M4 IT organization slowness	▪ Slow responsiveness/lacking agility ▪ Disadvantageous prioritization ▪ Long development/purchase times
		M5 Beneficial cost structure anticipation	▪ Lower cost than central solution/transaction costs ▪ Low initial costs
		M6 Business environment uncertainty	▪ Uncertain environment
		M7 Competence lack/resource scarcity in IT organization	▪ Lack of knowledge/competence ▪ Missing resources
		M8 BU power loss	▪ Loss of power of BU
	Missing barriers	**MB1** Restriction lack	▪ Lack of restrictions
		MB2 Awareness lack	▪ Lack of awareness
Outcomes	**Benefits**	**B1** Productivity gain	▪ General productivity/efficiency/effectiveness gain ▪ Employee productivity/efficiency/effectiveness gain ▪ Improved workflows/business processes
		B2 Innovation increase	▪ Innovation increase/creativity
		B3 Agility enhancement & flexibility increase	▪ Flexibility enhancement ▪ Agility increase
		B4 User/customer satisfaction improvement	▪ User/employee satisfaction ▪ Perceived higher quality of own applications ▪ Customer satisfaction
		B5 Collaboration enhancement	▪ Shadow IT instances fostering collaboration ▪ Enhanced collaboration during creation of Shadow IT
	Risks/short-comings	**R1** Security risks & lacking data privacy	▪ IT security/compliance threats ▪ Data privacy threats ▪ Regulation risks

Figure 7. Coding scheme used to identify and structure research themes

Category	Subcategory	Research theme	Keywords/phrases for coding
Out-comes (cont.)	**Risks/short-comings (cont.)**	**R2** Integration lack & data inconsistencies & architecture insufficiency	▪ Integration lack with existing systems ▪ Errors/inconsistencies ▪ Credibility loss/hindered decision making ▪ Architectural challenges
		R3 Synergy loss & inefficiency creation	▪ Synergies loss/standardization prevention ▪ Inefficiencies/redundancies ▪ Investment increase/resource waste
		R4 Control loss	▪ Control lack/governance harm ▪ SIT dependence ▪ Vendor dependence
		R5 Continuity lack	▪ Key personnel dependencies/missing documentation ▪ Low support risk ▪ Breakdown risk
Gover-nance	**General governance for Shadow IT and Business-managed IT**	**GG1** Policy setup	▪ IT policy design considerations ▪ Policy setup considering value of Shadow IT Allow Shadow IT in controlled manner ▪ Restrict critical Shadow IT
		GG2 Awareness training	▪ Awareness training
		GG3 IT systems gap resolution	▪ IT system gaps ▪ Closing gaps might not help
		GG4 Monitoring & identification	▪ Control considerations ▪ Technical monitoring ▪ Categorization overt/covert ▪ Shadow IT identification
	Instance governance for overt Business-managed IT	**IG1** Instance categorization	▪ Shadow IT types ▪ Categorization criticality/quality ▪ Functional scope/scope of use ▪ Other categorizations
		IG2 Instance decommission	▪ Instance decommission
		IG3 IT organization instance governance	▪ Instance responsibility transfer to IT/integration/replacement ▪ Criticality/quality assessment
		IG4-1 IT organization providing platform	▪ Provide general platform ▪ Provide architecture layer ▪ Provide data layer ▪ Provide service layer ▪ BYOD & enterprise app stores
		IG4-2 IT organization managing risks	▪ IT organization manages risks
		IG4-3 IT organization supporting implementation	▪ Continuous support ▪ Manage vendors ▪ Project management ▪ Service management ▪ Manage collaboration/knowledge exchange
		IG4-4 BU defining requirements/ designing application	▪ Define requirements ▪ Design application ▪ Perform tasks requiring specific business knowledge
		IG5 BU instance governance	▪ Limited scope/SaaS solution ▪ High business-specific skills needed

Figure 7. Coding scheme used to identify and structure research themes (continued)

Appendix B. Detailed coding results and research setup of literature items

Figure 8. Concept matrix of coding results and research setup of all literature items

Appendix C. Longitudinal analysis of research themes

					Received attention		
					⬆ Increase of coverage >5% until 2015/since 2016	➡ Coverage delta until 2015/since 2016 <=5%	⬇ Decrease of coverage >5% until 2015/since 2016	#% Coverage delta until 2015/since 2016 >15%

Category	Subcategory	Research theme	Over-all	Until 2015	Since 2016	Delta	
Causing factors	**Enablers**	E1 Technical accessibility	21%	19%	24%	⬆	6%
		E2 IT user competence	17%	19%	14%	⬇	-5%
	Motivators	M1 IT organization and BU non-alignment	41%	43%	38%	⬇	-5%
		M2 IT system shortcomings	41%	46%	32%	⬇	-13%
		M3 Employee motivation/impact orientation & peer behavior	30%	31%	27%	➡	-4%
		M4 IT organization slowness	21%	17%	30%	⬆	13%
		M5 Beneficial cost structure anticipation	19%	17%	22%	➡	4%
		M6 Business environment uncertainty	10%	4%	22%	⬆	17%
		M7 Competence lack/resource scarcity in IT organization	7%	6%	8%	➡	2%
		M8 BU power loss	4%	3%	5%	➡	3%
	Missing barriers	MB1 Restriction lack	12%	10%	16%	⬆	6%
		MB2 Awareness lack	8%	13%	0%	⬇	-13%
Out-comes	**Benefits**	B1 Productivity gain	33%	33%	32%	➡	0%
		B2 Innovation increase	25%	21%	32%	⬆	11%
		B3 Agility enhancement & flexibility increase	16%	13%	22%	⬆	9%
		B4 User/customer satisfaction improvement	11%	13%	8%	➡	-5%
		B5 Collaboration enhancement	9%	6%	16%	⬆	11%
	Risks/short-comings	R1 Security risks & lacking data privacy	33%	33%	32%	➡	0%
		R2 Integration lack & data inconsistencies & architecture insufficiency	28%	27%	30%	➡	3%
		R3 Synergy loss & inefficiency creation	26%	26%	27%	➡	1%
		R4 Control loss	22%	16%	35%	⬆	19%
		R5 Continuity lack	15%	11%	22%	⬆	10%
Gover-nance	**General governance for Shadow IT and Business-managed IT**	GG1 Policy setup	27%	23%	35%	⬆	12%
		GG2 Awareness training	11%	11%	11%	➡	-1%
		GG3 IT systems gap resolution	5%	4%	5%	➡	1%
		GG4 Monitoring & identification	22%	19%	30%	⬆	11%
	Instance governance for overt Business-managed IT	IG1 Instance categorization	22%	16%	35%	⬆	19%
		IG2 Instance decommission	3%	0%	8%	⬆	8%
		IG3 IT organization instance governance	16%	14%	19%	➡	5%
		IG4-1 IT organization providing platform	13%	7%	24%	⬆	17%
		IG4-2 IT organization managing risks	7%	3%	16%	⬆	13%
		IG4-3 IT organization supporting implementation	11%	6%	22%	⬆	16%
		IG4-4 BU defining requirements/designing application	7%	3%	16%	⬆	9%
		IG5 BU instance governance	11%	11%	11%	➡	-1%

Figure 9. Longitudinal analysis of research attention of individual research themes (the percentage of identified literature items mentioning themes in category and subcategory, 70 literature items until 2015, 37 items since 2016)

Biographical notes
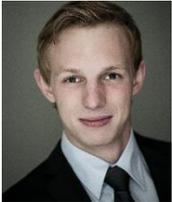
Stefan Klotz

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.

www.shortbio.net/stefan.klotz1@mailbox.tu-dresden.de

Andreas Kopper

PhD candidate at the Faculty of Business and Economics 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 is about Shadow IT and Business-managed IT.

www.shortbio.net/andreas.kopper@mailbox.tu-dresden.de

Markus Westner

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 acted 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.

www.shortbio.net/markus.westner@oth-regensburg.de

Susanne Strahringer

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 modelling.

www.shortbio.net/susanne.strahringer@tu-dresden.de