Perceptions of IT Managers on Shadow IT

Andreas Kopper
TU Dresden
andreas.kopper@mailbox.tu-dresden.de

Abstract

Shadow IT is the autonomous procurement or usage of IT by business units or users without involving the IT organization. To get an up to date IT management’s perspective on this phenomenon, 16 interviews with executive or senior IT managers were conducted. Using content analysis, the empirical data is compared with current themes about Shadow IT that were previously identified in a review of practitioner articles. In contrast to academic research, many practitioners currently deal with governance aspects of Shadow IT and its controlled use in organizations. We find that some study participants enable “Business-Managed IT” to harness the potential of Shadow IT in certain areas but also to manage associated risks. However, participants prefer to improve the IT organization to better serve their users and thus to reduce the need for Shadow IT.

Keywords
Shadow IT, Business-Managed IT, IT Governance, Agility, IT Security, IT Architecture

Introduction

Shadow IT includes all software (incl. Software/Platform/Infrastructure as a Service), hardware, or IT service processes which are used or created autonomously by business units (BUs) or users without alignment with the corporate IT organization (Kopper and Westner 2016b; Zimmermann et al. 2014). It is a phenomenon that is recently gaining more relevance in practice and also receiving increased academic attention (Kopper and Westner 2016a). One of the identified reasons for the increase of Shadow IT is the low barrier of deploying software and services through new cloud-based technology-delivery models. This makes BUs less dependent on the corporate IT organization and enables them to engage with vendors on their own (Andriole 2015). Similarly, decentral office application suites make it easy for users to build their own, sometimes sophisticated, solutions when they see their own operational efficiency hindered by shortcomings and inflexibility of official enterprise systems (Spierings et al. 2016). Another contributing factor for Shadow IT is dissatisfaction with or lack of IT organization’s support of BUs’ needs (Fürstenau et al. 2016).

Prior academic research has mostly dealt with the negative effects of Shadow IT. One of the risks of Shadow IT is a lack of integration with the remaining corporate IT landscape. This aspect usually has low priority when users are procuring solutions themselves but associated problems must often be solved later by the IT organization (Chua et al. 2014). Additionally, the resulting heterogeneous landscape makes standardization difficult (Huber et al. 2016) and can lead to increased costs through inefficiencies (Singh 2015). Other risks associated with Shadow IT are related to security shortcomings and together with data-related issues can have significant (regulatory) consequences for organizations (Gozman and Willcocks 2015; Kerr and Houghton 2008; Kretzer 2015; Silic and Back 2014).

Less research dealt with potential positive effects of Shadow IT (Zimmermann et al. 2017) and how it can contribute to innovation in organizations (Silic et al. 2016). Some recognize the phenomenon as an effective and efficient way to deal with shortcomings of corporate systems (Alter 2014; Behrens 2009) or as a way to rapidly react to quickly changing business requirements (Tambo and Bækgaard 2013).

Prior research also focused on causes, consequences, and governance aspects of Shadow IT. Especially governance aspects and potential positive aspects are overall least covered by the academic community (Kopper and Westner 2016a) but gaining attention recently. To complement academic views and to capture views on the topic that are as current as possible, Kopper et al. (2017) systematically analyzed 397
practitioner articles related to Shadow IT which were published over the course of one year. Consistent with the recent focus in academic research, many practitioner articles dealt with governance aspects of Shadow IT. A theme that emerged and which is still underrepresented in academic research is the controlled use of Shadow IT in organizations. Although the phenomenon of Shadow IT has been picked up in a lively academic discourse, there is still a limited understanding of actual organizational practices regarding Shadow IT.

While the review by Kopper et al. (2017) was rigorously conducted from a methodological perspective, practitioner articles as a data source might bias study results. Therefore, the study at hand aims to further examine and validate the findings of the literature analysis (referred to as “review” for the rest of the paper at hand) by comparing them with empirical data. For that, exploratory interviews with 16 executive/senior IT managers (or business managers with a close link to IT) in the DACH region (Germany, Austria, and Switzerland) were conducted to capture their perspectives on Shadow IT. In light of this, the paper at hand aims to answer the following research questions: (RQ1) What is the current perspective of IT managers (or business managers with a close link to IT) on Shadow IT, especially in regard of organizational practices? (RQ2) How does this perspective match current views represented in practitioner articles?

The rest of the paper is structured as follows: First, the research methodology is described, then the results are reported, followed by a summary including discussion, and ending with the conclusions, limitations, and an outlook on future research.

Methodology

Overall 16 interviews (Table 1) with senior or executive IT managers or business managers with a close link to IT were conducted. The selection of participants focused on medium and large companies from different industries which have distinctive organizational structures (for example a separate IT organization). To reduce linguistic misunderstandings and cultural differences, the selection concentrated on companies from German-speaking countries. After a pilot interview (Yin 2003) in July 2016, the remaining ones took place from October 2016 to February 2017. A qualitative research approach was selected to gain an adequate understanding of the complex aspects involved and to be able to identify details which help to further deepen understanding of contextual factors (Yin 2003). Using multiple interviews made it possible to cover a broad company spectrum regarding industries, organizational setups, and sizes. Interviews are an appropriate data gathering approach because Shadow IT is deemed as a highly sensitive topic which requires a high degree of trust between the interview partners to talk about it. Not only has the term itself a negative connotation, but one of the main causes for Shadow IT is shortcomings of existing IT systems (Kopper and Westner 2016a) which usually lie within the responsibility of the interviewees. Personal recommendations and non-disclosure agreements in advance of the interviews supported trust building from a social and legal perspective.

Before each interview, a written survey was sent to the participants to gather descriptive company data such as revenue and number of IT users. The interviews lasted one hour on average and were recorded. One interview was conducted on-site and the other ones as video or audio conferences. Following suggestions from Myers and Newman (2007) and Yin (2003), semi-structured interviews with open questions were used. This allowed the participants to speak freely about their experiences and perceptions and allowed flexibility to pursue new topics. The open questions aimed at: 1) Understanding of organizational structure and context, 2) Discussing positive occurrences of Shadow IT, and 3) Discussing negative occurrences of Shadow IT. The predefined structure was limited to those three sections instead of closely following the concepts of the framework created by Kopper et al. (2017) to allow flexibility and avoid confirmation bias.

For detailed follow-up questions, improvisation and listening strategies were used (Myers and Newman 2007) to get an understanding of the respective organizational and technical context.

The audio recordings were transcribed, anonymized, and sent to participants for approval. The transcripts were then coded (Corbin and Strauss 2008) using MAXQDA. The concepts of the framework shown in Figure 1 were used as an initial coding scheme. For identification of additional (sub)categories, guidelines for open coding were used (Corbin and Strauss 2008). The codes were then analyzed for each interview and re-mapped to the concepts in Figure 1. A second researcher selectively reviewed the codes in multiple iterations.
Results

Overview

Figure 1 shows current themes regarding Shadow IT as discussed in practitioner literature (Kopper et al. 2017) and to what extent the underlying concepts could be confirmed by the collected empirical data. The framework describes (A) environmental pressure on the IT organization in the form of Shadow IT which exists due to unaddressed user needs. (B) This requires the IT organization to adapt and better meet the users’ expectations. A way to cope with the issue is to make controlled use of Shadow IT by (C) enabling, but also (D) securing it. (E) A possible trend of this decentralized approach could change the future role of the IT organization within the enterprise.

Table 1 shows the study participants (in chronological order of the interviews) and the individual mapping of the interview results to the concepts in Figure 1.

<table>
<thead>
<tr>
<th>ID</th>
<th>Participant</th>
<th>IT users</th>
<th>Industry</th>
<th>Pressure on IT</th>
<th>Impact on IT</th>
<th>Controlled use of Shadow IT</th>
<th>Reorientation of IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>P01</td>
<td>CIO</td>
<td>&gt;20,000</td>
<td>Engineering Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a service provider and strategic partner</td>
</tr>
<tr>
<td>P02</td>
<td>CIO</td>
<td>&gt;2,000</td>
<td>Electronic Equipment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a service provider and strategic partner</td>
</tr>
<tr>
<td>P03</td>
<td>Senior IT mgr</td>
<td>&gt;10,000</td>
<td>Machinery</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P04</td>
<td>Senior IT mgr</td>
<td>&gt;40,000</td>
<td>Commercial Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P05</td>
<td>CIO &amp; CFO</td>
<td>&lt;500</td>
<td>Energy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P06</td>
<td>CIO</td>
<td>&gt;10,000</td>
<td>Financial Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P07</td>
<td>CIO</td>
<td>&gt;5,000</td>
<td>Electrical Equipment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P08</td>
<td>CIO</td>
<td>&gt;5,000</td>
<td>Public Sector</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P09</td>
<td>CIO</td>
<td>&lt;500</td>
<td>Utilities</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P10</td>
<td>CIO</td>
<td>&gt;5,000</td>
<td>Health Care</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P11</td>
<td>DTO</td>
<td>&gt;20,000</td>
<td>Health Care Equipment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P12</td>
<td>CIO</td>
<td>&gt;2,000</td>
<td>Wholesale</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P13</td>
<td>CIO</td>
<td>&gt;20,000</td>
<td>Insurance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P14</td>
<td>Senior IT mgr</td>
<td>&gt;5,000</td>
<td>Health Care</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P15</td>
<td>CIO</td>
<td>&gt;5,000</td>
<td>Electronic Equipment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
<tr>
<td>P16</td>
<td>CIO</td>
<td>&gt;100,000</td>
<td>Transportation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>IT as a cloud broker</td>
</tr>
</tbody>
</table>

Table 1. Study participants and mapping of results to the concepts in Figure 1.
Perceptions of IT Managers on Shadow IT

Pressure on IT

(A) Higher market requirements and user expectations

“Age of disruption” Disruption describes a process where innovations create new markets and threaten established incumbent companies. However, none of the participants mentioned a risk of their business to be disrupted and therefore being under increased external market pressure. Only one participant (P09) indicated increased competition due to current market dynamics and/or opportunities. The other participants faced “classical” challenges such as inefficiencies due to heterogeneous systems, legacy systems, generally slow processes, and scarce resources.

Shadow IT All participants except for two admitted that Shadow IT exists or existed in their organizations. The occurrences of Shadow IT range from small, sophisticated “spreadsheet applications” to large shadow systems covering critical business processes. However, due to the usually hidden nature of Shadow IT the participants could not tell its precise extent.

Consistent with the review by Kopper et al. (2017), participants often mentioned risks related to security (88%) and poor integration of solutions in the existing IT landscape (69%) as well as risks such as increased costs and project timelines getting out of hand, especially for large projects. Ironically, the two most prominent reasons for BUs to “go alone” without involving the IT organization is the perception that the IT organization is too slow or too expensive (P01, P03, P06, P07, P13, P14).

One participant (P04) mentioned having no significant (prior) cases of Shadow IT due to the decentralized nature of his/her organization and indicated that IT managed in the BUs themselves is “business as usual”. A second participant (P12) has a very strict “command and control” type of organization which completely prevents Shadow IT from his/her perspective.

Impact on IT

(B) IT organization needs to adapt

Agile organization Most participants recognized the importance of their IT organizations to become more agile or generally to react faster to the requirements and needs of their business users (IT users within BUs). 63% of the participants admitted that business users perceive the provided IT services as being slow or that users are dissatisfied because solutions do not meet their requirements.

Remarkably, none of the participants identified their organization as working fully agile. The descriptions ranged from being “still at the beginning of the journey” (P02) to “introduced agile 1 ½ years ago […] but we are just starting to involve the [business] customer in the development process” (P13). Some organizations have faster, separate processes for smaller requirements (P08, P10, P14). One step further, one organization implements small enhancements very quickly in an agile way closely hand in hand with business users and with as little process overhead as possible (P07). Another organization established a separate agile team to be able to rapidly react in areas with fast changing requirements (P13).

A common theme with broad agreement was also that business-IT alignment needs to be improved and that it is an important factor to prevent Shadow IT. This mainly involves better, closer, more informal communication between BUs and IT (P01, P05, P07, P09, P11, P13, P16). Participants wish for a higher level of trust and routine that encourages users to involve the IT organization early for their IT needs and to seek advice. Even though this requires effort from both sides, the IT organization can actively keep in close touch with BUs and can ensure that IT staff has the right skills and business process knowledge to act as trusted advisors (P05, P13). For some participants, “key users” are an important link between IT and BUs (P10, P11, P12). They usually reside in the BUs, have strong process knowledge, at least basic IT knowledge, and keep close contact to the IT organization.

A theme that emerged but was not identified in the review by Kopper et al. (2017), was the importance of a mature (and agile) demand management process as an instrument to both react faster to user requests and to improve business-IT alignment (P03, P04, P12, P13, P15). To increase efficiency, demand can also be pre-prioritized by key users directly in the BUs before discussing it centrally (P12). Independently of how long a request would take to fulfill, users should receive fast feedback and a comprehensible explanation in case their request needs to be denied, for example due to security concerns (P05).
Kopper et al. (2017) mentioned the positive notion of using Shadow IT to identify user needs. This aspect could not be found in any of the interviews. Only one participant emphasized the need to proactively investigate new solutions in order to offer alternatives early to prevent Shadow IT (P09).

**Modern IT architecture** Some participants mentioned the direct influence of IT architecture on their ability to be fast and agile: “We are working agile […] but it very much depends on the [IT] system” (P13, similarly also P11). For example, P11 mentioned that in his/her organization there are 12 releases per month in a Salesforce environment and only 2 to 3 per year in an on-premise SAP environment. Some emphasize the importance of cloud-based delivery to achieve high speed and agility (P01, P04, P10, P11).

Public cloud offerings are not yet embraced in the participants’ companies on a broad scale, except in one case (P11). Issues around privacy, security, and regulatory difficulties still hinder broader adoption even if some participants recognize the advantages and expressed a desire to endorse it more explicitly (P01, P09). More frequently observed were private cloud models by running an own datacenter (P09, P14, P15, P16) or using an outsourced, dedicated infrastructure which is managed up to the operating system layer (P10, P13).

There seemed to be a trend in the participants’ organizations towards standardizing and abstracting from infrastructure, spending less resources on the lower levels of the software stack, and concentrating more on the application layer. Some of them mentioned current standardization efforts (P02, P04, P05, P08, P10) and are still plagued by “old” problems dealing with historically grown heterogeneous landscapes and legacy systems. This issue was not identified by Kopper et al. (2017) as a hindering factor but is more prominent for the participants than any other issue. One participant was faced with the task to consolidate >1,000 applications (originating from several mergers in the past) to be able to standardize the application landscape and the IT service processes and to increase efficiency while also centralizing the underlying infrastructure (P16).

These issues could be the reason why only two participants partially mentioned higher modularization (of monolithic systems) as a measure for more flexibility (P01, P13) although modularization was frequently mentioned by the experts in the review by Kopper et al. (2017). However, for two participants, system changes are very time consuming and complex due to highly integrated systems and processes (P12, P15). Two other participants are currently introducing integration services (for example, Enterprise Service Bus) to achieve higher flexibility (P06, P11).

**Controlled use of Shadow IT**

**(C) Enable Shadow IT**

**Support implementation** Some participants point out the advantage of Shadow IT to directly make use of deep process knowledge in BUs (P02) and potentially being more flexible and faster (P04) compared to IT-led initiatives. However, views on the topic and corresponding organizational setups are different. Some have or target very centralized, IT dominated organizational setups (P01, P12, P14) while others are comfortable with a decentralized organizational setup where BUs take over large parts of IT responsibilities (P02, P04).

Some participants follow a vertical split of responsibilities where BUs potentially cover multiple layers of the stack for specific systems. This involves BUs being predominantly responsible for IT that is embedded in or related to tangible customer products, IT products/services directly offered to customers, or IT that is related to manufacturing (P02, P04, P15). Referring to that, one participant noted: “This [specific] knowledge only exists in the BUs. For me, IT would only be a bottleneck here.” (P02). Another possibility is to split responsibilities for projects involving emerging technologies and unstable requirements (P15), to engage with local BUs for proof of concepts, or BUs taking care of local customer facing systems (P16). Others accept or tolerate if BUs only develop small applications that do not require deep integration with the IT landscape (P07, P13). Horizontal splits where the IT organization is taking over the infrastructure/platform levels of the system stack and BUs the application layer, are separately described in the next section.

There is broad agreement among participants that a strong, mature governance is required for Shadow IT to work. One participant noted: “I’m a big fan of decentralized IT […] but it needs to be embedded in a central governance” (P16). All of the examples describe some form of central authority to coordinate central/decentral and global/local initiatives to ensure efficiencies. They include an “overarching project...
portfolio management” to keep an overview of small scale initiatives (P11), a “neutral demand management” that makes sure that synergies are reached by distributing BU-specific solutions that might be beneficial for other BUs (P06), and a “project portfolio review board” where global and local initiatives are reviewed and aligned regularly (P16). Still, the governance process should not be too rigid to allow for some flexibility (P15, P16).

Beyond coordination of initiatives, participants also point out the importance of involving the IT organization as early as possible to mitigate possible risks. That might happen in an “architecture board” which evaluates the overall fit of the solution, the impact on the existing IT landscape, integration, and security aspects (P07). Strict regulatory requirements in industries such as financial services can also require a minimum of documentation, versioning, testing, and user authorization which may be difficult to cover by BUs themselves (P06).

Participants frequently pointed out that vendor management should still be the responsibility of the IT organization (P03, P06, P15, P16). Vendors might later directly work with the BUs, but the IT organization should at least be involved in the vendor selection phase and use its experience to make sure that the right vendor is selected, that costs are under control or negotiated appropriately, and that the vendor receives all necessary information about standards such as integration and security aspects (P13, P16).

Identified in the review by Kopper et al. (2017) but only rarely mentioned in the interviews was direct support for Shadow IT by the IT organization in the implementation process. Examples include providing technical expertise for infrastructure design (P02), coaching of Salesforce developers in BUs to retain consistent data models and workflows (P11) or general expert support for difficult implementation issues (P11). Only one participant indicated that his/her IT organization was providing development environments and standardized tool support (P06). However, nobody mentioned providing a catalogue of tested and sanctioned third party cloud applications.

**Provide platform** As mentioned before, from a technical perspective, there is also the possibility to vertically split responsibilities of IT and business in the system stack. On the lowest layer, the IT organization can provide secure and controlled infrastructure for Shadow IT (P06, P15) or local proof of concepts (P16). That way, at least on the infrastructure layer, a level of standardization, control, security, and cost/scale benefits can be assured (P04).

The next level of abstraction includes providing and standardizing the data layer as well. That would mean managing, e.g., databases or (the data layer of) ERP systems in the IT organization and providing access for Shadow IT (P04). This further ensures standardization and fosters integration of systems. More common is providing access to a central data repository in a more restricted way in order to enable the flexible creation of reporting solutions in BUs, utilizing the subject-specific process knowledge (P07). By having direct (read only) data access and being able to create queries, business users are ensured to receive up to date and consistent information. Based on that, they can separately process data in spreadsheet solutions in a flexible way for temporary requirements. If a long-term requirement emerges, they need to trigger a centrally managed, iteratively developed system change to retain consistency (P05).

A similar example involves providing a self-service data integration platform where the IT organization is managing the technical integration layer with existing systems. Using the platform, business users are able to consolidate data for reporting purposes from multiple systems or potentially integrate new applications with a simple drag and drop interface (P06).

In one instance, Salesforce is used as a platform for business users to build their own reports, dashboards, and workflows (P11) and another participant (P06) started implementing such a setup. By that, the platform removes the complexity of the underlying application and infrastructure layers. This reduces the required technical expertise and allows certain skilled business users ("champions") familiar with the business processes to make fast, flexible adjustments. Interestingly, this platform emerged as an unsanctioned shadow system years ago before it was taken over centrally and reworked into a successful official system.

None of the participants used, but two described the idea of a “low code” environment as mentioned by Kopper et al. (2017) for future use (P07, P11). This would strongly abstract the system stack from the business user and would allow implementation of applications without software development knowledge. Two could imagine a possible horizontal split by providing a platform sometime in the future but are currently not in a state to do so (P02, P09).
(D) Secure Shadow IT

Manage IT security and risks  Security issues or in general risks related to Shadow IT were frequently occurring topics during the interviews. They are partially covered by the “governance” aspect in the previous section “Support implementation” but discussed separately here due to their prominence. There needs to be a policy to define the boundaries of Shadow IT, i.e., what “official” or “not official” actually is. Disciplinary enforcement makes it possible to honor that split of responsibilities (P01). For example, spreadsheet solutions could be denied by the CFO when SAP usage is mandatory (P05) or central support denied for spreadsheet solutions (P12). To be able to decide which services are allowed and not allowed, the IT organization also needs to be fast in evaluating quickly spreading Shadow IT solutions such as WhatsApp and potentially offer alternatives (P04, P05).

Policies for Shadow IT can cover general (regulatory) compliance, licensing, security, and privacy requirements that need to be met. In four cases, it is a cross-divisional task that is taken over by the IT organization to ensure these aspects when responsibilities are split with BUs (P02, P04, P06, P07). An early involvement of the IT organization should be considered to adhere to these aspects already from the design phase. As one participant pointed out, a security concept is “not just a piece of paper” and not something that can be just added at the end of a project (P08). Especially in highly regulated industries it can be very difficult to meet all the requirements in Shadow IT projects when additional regulatory requirements such as public procurement laws are involved (P08).

To make sure that BUs and users adhere to these policies, participants try to increase awareness by close and repeated communication. Close contact with BUs also helps retaining high visibility of solutions used and to potentially identify Shadow IT (P05, P14). Also, security related rejections of requests should be communicated in a comprehensive way so that business users are still willing to collaboratively find an alternative solution (P05). No participant mentioned using disciplinary consequences for violating policies related to Shadow IT, but one is using direct, individual confrontation/discussions as an effective measure to enforce them (P12). Part of managing the risks related to Shadow IT is also to evaluate, to prioritize, and to take over existing identified solutions to ensure security standards (P01, P03, P08, P13).

Protect data and infrastructure  Gaining full visibility of Shadow IT is difficult for most participants. Some even mentioned that it is generally inevitable and it is not possible to suppress it with absolute certainty. However, visibility on a technical level is important to be able to enforce previously defined policies. This could include identifying unsanctioned network devices which pose a security risk (P03, P04) or even unofficial servers residing in the BUs.

None of the participants mentioned using a so-called Network Access Security Broker which was identified in the review by Kopper et al. (2017) as a tool for network monitoring and access control to cloud services. The most common measure on network level was blocking specific cloud services such as Dropbox or Amazon Web Services, but there was no network monitoring in these cases to identify Shadow IT (P03, P10, P12, P13, P14). Participants who perform active network scanning do so primarily for general security reasons, not especially for identifying Shadow IT (P04, P16). Mentioned by some was endpoint security/monitoring to gain visibility of or block installation of illicit applications on user devices (P04, P12, P14).

In contrast to the review, none of the participants mentioned the topic of encryption in connection with protecting data and infrastructure. However, one theme that emerged was ensuring security and visibility by standardizing infrastructure. One participant described a high level of visibility of shadow systems because BUs would need to request secure server resources from the IT organization first due to the centralized infrastructure setup and locked down network (P07). P04 explained the benefits of having a standardized infrastructure in the organization with an analogy to large, public IaaS providers. Like the IT organization for BUs, these vendors offer infrastructure to their customers and can ensure strong security mechanisms through standardization, scale, and having the resources to apply appropriate expertise (P04).

Reorientation of IT

(E) The new role of the IT organization within the enterprise

The review by Kopper et al. (2017) deals with potential implications of the themes discussed in (B) “Impact on IT” and (C)/(D) “Controlled use of Shadow IT” on the future role of the IT organization within the
enterprise. Because this is a perspective view which is very dependent on individual assessments, it cannot be confirmed in the same form as the previous themes but is briefly discussed in the next section.

Summary and discussion

Shadow IT is (or was) a common issue for the participants but the individual perceptions of it vary. One of the main identified countermeasures is to prevent Shadow IT by targeting some of its root causes (Fürstenau et al. 2016). Another one is that IT organizations should become more agile to be able to deliver faster (Györy et al. 2012) and to be more closely aligned with BUs (Winkler and Brown 2014b). The reason for the lack of general organizational agility could be the large size and age of most of the participants’ companies (Hannan and Freeman 1984). A related measure is to maintain a good business IT alignment and to improve the sometimes conflicted relationship between both entities. Only one participant pointed out a necessary increase of resources for the IT organization (Winkler and Brown 2014a) as being most important to better fulfil requests and therefore prevent Shadow IT (P03). Another one identified lacking IT resources at least as a contributing factor (P05).

Participants also confirmed the importance of IT architecture on their ability to operate in an agile way and to be able to fulfil requests quickly. While there was agreement that utilization of cloud technologies is an essential factor (Rockmann et al. 2015), only one of the participants (P11) used a significant amount of public cloud services and private cloud deployments were more common. Another factor that emerged was standardization of heterogeneous infrastructure and legacy systems as a measure for more efficiency (regardless of whether cloud technologies are used or not).

Some participants have a positive view on Shadow IT if it is subject to certain conditions. IT managed by users or BUs themselves mainly involves giving departments responsibility for product-related IT (R&D), IT in production processes or small, non-critical solutions that do not require deep integration (Fürstenau and Rothe 2014; Winkler and Brown 2014b). Still, this requires a strong, central governance (Györy et al. 2012) and the IT organization should be involved in or remain responsible for vendor management (Chua and Storey 2016). Also, the split of responsibilities (Chua et al. 2014; Winkler and Brown 2014b; Zimmermann et al. 2016) should be clearly defined (P04). Notably, no participant plans to have more decentralization, but rather some are consolidating infrastructure or core systems (P04, P05, P06, P10).

Although there are positive manifestations of Shadow IT, the negative connotation of the term Shadow IT is in contrast with its potential positive effects. Therefore, we suggest a differentiation between Shadow IT and Business-Managed IT similar to “Business-Driven Solutions” (Györy et al. 2012) and “Business-Located IT” (Zimmermann et al. 2016). Kopper et al. (2017) already pointed out the necessity for using a separate term and it became clear during the data gathering phase of this study that the following differentiation based on the participants’ views is required: While both terms can have many similarities and overlaps, Business-Managed IT in contrast to Shadow IT is involved in the organizational IT management. It is therefore based on an agreed upon split of responsibilities between the (centralized) IT organization and the (decentralized) BUs. It is different from the related term “End-User Computing” (Panko and Port 2012) by including BUs in addition to individual users and also large scale IT artifacts of various types (e.g., SaaS). It is furthermore focused on long-term solutions in comparison to short-term “Workarounds” (Alter 2014).

One participant pointed out that a high degree of centralization is necessary to be able to provide a standard environment for Business-Managed IT (P07). A common infrastructure, data or platform layer would ensure a minimum degree of standardization, integration, and security, and would decrease the complexity or required skills for Business-Managed IT initiatives (Sedera et al. 2016; Yoo et al. 2012). At its most abstract form, users could develop and integrate applications on a “low code” platform (Beimborn et al. 2011; Krancher and Luther 2015) but none of the participants currently use such an environment. Closest to this idea is the example of users being able to adapt their own systems on Salesforce (P11).

Next to integration issues, security concerns were a popular theme related to both Shadow IT and Business-Managed IT during the interviews. Compliance requirements should be clearly defined in a policy and awareness created by close communication with users (Haag and Eckhardt 2014; Puhakainen and Siponen 2010). For participants who split responsibilities in certain Business-Managed IT initiatives, the IT organization takes over the security cross section. To de-risk existing Shadow IT, participants also shut down or integrate/reengineer solutions where appropriate. The decision on whether to legitimize, more closely monitor or take over these solutions can be made based on their risk level (Zimmermann et al. 2017).
To enforce policies on Shadow IT, participants use network and endpoint level blocking based on blacklists. However, active network scanning and analysis is rarely used in practice. Even if, identification of Shadow IT is only a byproduct of security measurements in these cases. Identifying all types of Shadow IT (devices, cloud services, etc.) to have full transparency is generally deemed important, but difficult for participants.

Related to the themes previously discussed, the review by Kopper et al. (2017) also deals with their potential implications on the future role of the IT organization within the enterprise. A continuous trend towards IT autonomy in the BUs could decrease the relevance of the IT organization and force it to operate more as a service provider and strategic partner for the business, less focusing on technology management. It could also be reduced to a mere cloud broker if BUs will source all their systems from the public cloud themselves at some point in the future. Those scenarios could not be confirmed in the interviews or only to a minimal degree, but they could probably emerge as a desired “organizing vision” (Swanson and Ramiller 1997) when involving business users without IT background in the discussion.

Conclusion, limitations and future research

The study revealed different perspectives on Shadow IT and related organizational practices (RQ1). A possible opposing strategy to deal with Shadow IT is to prevent it by utilizing control mechanisms or by addressing its root causes through improvement of the IT delivery mechanisms. Another, though less popular strategy revealed in the study is to make controlled use of Shadow IT or Business-Managed IT as currently discussed in practitioner articles (RQ2). The paper contributes to the body of research by describing actual organizational practices around Shadow IT based on a larger set of different companies. Those can also help practitioners in their decision making process on how to deal with Shadow IT. A conceptual contribution lies in the introduction of the concept Business-Managed IT which can help getting a better and nuanced understanding of the phenomenon.

A limitation of this study is that it was conducted primarily with IT decision makers. There could be different aspects on the topics discussed from a (decentral) BU perspective (Andriole 2015). Another limitation is that all participants were from the DACH region and geographic specifics could have an influence on the results, e.g., related to usage of public cloud (due to security and privacy concerns) or preferences for integration/centralization. The latter was also pointed out specifically by P01. Additionally, as the focus of the study is on medium and large companies, the results may not apply in the same way to small ones.

Future research could deal with the further delineation of the term Business-Managed IT on a conceptual level, e.g., on the differentiation from Shadow IT and other forms of IT provisioning in BUs. Another possibility is to focus on the question under which circumstances Business-Managed IT is beneficial to organizations and how its risks can be mitigated. Also, further research is required on the possible future role of the IT organization in the enterprise.

References

Perceptions of IT Managers on Shadow IT


