Two Tales of Technology: Business and IT Managers' Technological Frames Related to Cloud Computing

Completed Research Paper

Sabine Khalil
Télécom ParisTech
46 rue Barrault, 75013 Paris
France
sabine.khalil@telecom-paristech.fr

Till J. Winkler
Copenhagen Business School
Howitzvej 60, 2000 Frederiksberg
Denmark
tw.digi@cbs.dk

Xiao Xiao
Copenhagen Business School
Howitzvej 60, 2000 Frederiksberg
Denmark
xx.digi@cbs.dk

Abstract

While cloud computing is becoming a mainstream IT sourcing option, especially large companies struggle with the internal governance of cloud and the issue of shadow IT. This study takes a technological frames perspective to contrast the knowledge and expectations that business versus IT stakeholders have regarding cloud IT. Our interview data from 20 business and IT managers display the incongruences between these two groups' technological frames and how this relates to their governing actions: While business managers emphasize the benefits frames of cloud computing and tend to undermine IT governance, IT managers stress its threat frames and their desire to strengthen the IT governance framework. We discuss how these frame incongruences are related and how they can be resolved. This discussion contributes to the literature a stakeholder-specific view that may help understand the duality of the shadow IT phenomenon. Theoretical and practical implications are discussed.

Keywords*:* Cloud computing, Business and IT managers, Technological Frames, Shadow IT, Interpretive qualitative study

Introduction

Cloud computing technology is becoming the mainstream option for sourcing IT application and infrastructure services. Market researchers forecast more than $132 billion in software as a service (SaaS) sales by 2020 and more than $55 billion in infrastructure (IaaS) and platform as a service (PaaS) revenues (ITA 2016). By 2020, the corporate 'no cloud' policy is considered to be as rare as today's 'no Internet' policy (Gartner 2016). Despite this clear trend, companies, especially large ones, struggle with the question on how to deal with the growing proliferation of cloud technology from an internal IT governance perspective (Andriole 2014; Winkler et al. 2014). Given that business departments can fairly easily implement and use cloud technology outside the radar of corporate IT departments, this trend

increasingly leads to the proliferation of what has been referred to more widely as 'shadow IT' (Behrens 2009; Walters 2013).

The academic literature has broadly studied the potential benefits and threats of organizational cloud computing adoption along various categories—the most frequently cited benefits relating to economics, scalability, agility, and ubiquity (e.g., Chebrolu 2011; Rajendran 2013; Zhang et al. 2010) and the most commonly mentioned threats relating to security, compliance, and reliability (e.g., Dutta et al. 2013; Onwubiko 2010; Srinivasan 2013). Underrepresented on this list of potential benefits and threats, however, are the issues related to the internal governance and control of cloud IT, which are often associated with the presence of shadow IT (Winkler and Brown 2014; Khan et al. 2016).

The emerging literature on shadow IT (Kopper and Westner 2016) suggests there is a duality around the shadow IT phenomenon in the sense that it can be both seen as a threat for corporate IT security (e.g., Behrens 2009; Walters 2013), but also as a benefit in terms of business productivity and innovation (e.g., György et al. 2012; Jones et al. 2004). What is also missing from the existing discussion on cloud computing is a differentiation of the perspectives of different stakeholders. For instance, when reviewing characteristics of cloud computing (or desires as called by the authors), Venters and Whitley (2012) separated the technological dimension from the service dimension, and hence advocated for more nuanced understanding of cloud computing.

In this paper, we focus on the cloud computing phenomenon by investigating the perceptions of the two stakeholder groups most pertinent to the organizational adoption of cloud computing: business managers and IT managers. Building on the notion that organizational change is a process in which people act on their own interest and interpretations of the world (e.g., Weick 1979; Pinch and Bijker 1984; Orlikowski 1996), this study draws on the theoretical lens of technological frames (e.g., Orlikowski and Gash 1994; Davidson 2006; Young et al. 2016) to dissect the differences in how these two social groups perceive cloud computing, and the consequences of such differences. Adopting the definition of technological frames as "knowledge and expectations that guide actor's in their interpretations and actions related to IT" (Davidson 2006 p. 24), we ask: *What are differences of business and IT managers' technological frames related to cloud computing?*

To address this exploratory research question, we conducted a series of 20 interviews with business and IT managers at large organizations and assessed their benefits and threat frames related to cloud computing using deductive and inductive qualitative research techniques. Our findings exhibit the ways in which the two groups emphasize different benefits frames and threat frames related to cloud computing: While business managers make sense of cloud computing primarily as a technology that brings about performance, agility, and ubiquity benefits, IT managers' views are dominated by the perception of the cloud computing's security, compliance, and reliability threats. These differences translate into frames related to the governance and control of cloud computing technology, which emerged from our analysis: Business and IT managers have a blatantly different understanding of how governance of cloud IT is practiced, and how it should be defined.

Overall, our results shed light on the two distinct stories that business and IT managers have developed to attribute meaning to cloud computing technology, and we discuss how this meaning influences their action and power in organizational realities. These findings contribute to the literatures on cloud computing and shadow IT, in that our technological frames perspective can help explain some of the duality revealed in the prior literature on governance of cloud computing and shadow IT. We also discuss theoretical implications for the technological frames perspective, outline practical implications, and point out opportunities for future research.

Literature Review

To provide us with an initial framework for our research on business and IT stakeholder perceptions, we review the cloud computing and shadow IT literatures, and explain the technological frames perspective.

Cloud Benefits and Threats

As cloud computing services are maturing, the academic literature has identified a number of benefits and threats related to their adoption. The following synthesis is based on a structured review of the literature

Table 1. Cloud benefits prevalent in the literature

Category	Benefits
Economics	• Economies of scale for providers (e.g. Onwubiko 2010; Srinivasan 2013) • Reduced training costs (e.g .Zhang et al. 2010; Yeboah-Boateng and Essandoh 2014) • Low price (e.g. Armbrust et al. 2010; Benlian and Hess 2011; Zhang et al. 2010) • Variabilization of costs (e.g. Onwubiko 2010; Wei et al. 2009) • Lower electricity consumption (e.g. Dutta et al. 2013; Yeboah-Boateng and Essandoh 2014) • Easy entrance for start-ups and SMEs (e.g. Srinivasan 2013; Yeboah-Boateng and Essandoh 2014) • Easy entrance for developing countries (e.g. Marston et al. 2011; Goundar 2010)
Scalability	• Computing resources on demand (e.g. Buyya et al. 2009; Tiers et al. 2014) • Scale up and down dynamically (e.g. Joha and Janssen 2012; Onwubiko 2010) • Minimal interaction with CSPs (e.g. Brynjolfsson et al. 2010; Rajendran 2013)
Performance	• Good quality of services (e.g. Benlian and Hess 2011; Dutta et al. 2013; Vishwakarma 2012) • Improved productivity (e.g. Armbrust et al. 2010; Rajendran 2013) • Robust machines and services offered (e.g. Buyya et al. 2009; Vishwakarma 2012)
Innovation	• New applications and services (e.g. Kundra 2011; Marston et al. 2011) • Lower IT barriers to innovation (e.g. Kundra 2011; Marston et al. 2011) • New markets (e.g. Brynjolfsson et al. 2010; Srinivasan 2013)
Agility	• More agile processes (e.g. Kundra 2011; Rajendran 2013) • Time-to-market (e.g. Chebrolu 2011; Yeboah-Boateng and Essandoh 2014)
Utilization	• Easy access for users (e.g. Rajendran 2013; Zhang et al. 2010) • Optimized resource utilization (e.g. Chebrolu 2011; Joha and Janssen 2012)
Ubiquity	• Ubiquitous access data and service: anywhere, anytime, anyway (e.g. Vishwakarma 2012; Zhang et al. 2010)

on cloud computing using the Sciencedirect and Ebscohost databases and keywords 'cloud computing', 'software as a service', 'platform as a service', 'infrastructure as a service', including forward and backward search techniques. In the style of a concept-centric review (Webster and Watson 2002) all retrieved papers were scanned and assigned to appropriate categories of benefits and threats (total of 27 papers).

The different cloud benefits found in the literature are displayed in Table 1. A number of references highlight the cloud's ***economic*** benefits stemming from economies of scale in providing IT services from large datacenters (Armbrust et al. 2010; Chebrolu 2011; Kundra 2011), from lower needs of functional staff and in-house expertise (Yeboah-Boateng and Essandoh 2014; Zhang et al. 2010), as well as from low maintenance fees (Dutta et al. 2013; Sultan 2011). Authors also emphasize that the pay-per-use characteristic of cloud computing allows users to pay only the amount of computing resources consumed (Onwubiko 2010; Wei et al. 2009). According to this view, cloud computing offers organizations cost-effective solutions that allow them to vary their costs through switching capital expenditures with operational expenditures (Marston et al. 2011; Zhang et al. 2010). Related to financial benefits, cloud computing is also considered a green computing alternative, since it uses less hardware on premises, supports lower carbon emission, and has lower electricity consumption (Dutta et al. 2013; Yeboah-Boateng and Essandoh 2014). Cloud services can provide an affordable entrance and access to IT for start-ups and SMEs (small and medium enterprises) that are otherwise not able to afford large hardware fees (Marston et al. 2011; Srinivasan 2013), as well as for organizations in less developed countries (Marston et al. 2011).

As mentioned by several researchers, cloud computing is highly ***scalable***, allowing organizations to allocate computing resources on demand (Benlian and Hess 2011; Chebrolu 2011; Onwubiko 2010), as well as to dynamically scale up or down with minimal interaction with cloud service providers (CSPs) (Armbrust et al. 2010; Marston et al. 2011). Some authors argue that cloud technology can increase an organization's ***performance*** through a good quality of services (Buyya et al. 2009), robust virtual machines (Vishwakarma 2012), and improved productivity (Rajendran 2013). Kundra (2011), Martson et al. (2011) and Yeboah-Boateng and Essandoh (2014) state that cloud computing can lead to different forms of ***innovation,*** since it supports the digitization of business processes, where the required number of steps along with the number of documents are decreased in each digitized process. For instance, cloud computing can enable new classes of applications (such as mobile applications, parallel batch processing, business analytics, IoT, etc.) (Kundra 2011), lowers the IT entry barriers (Marston et al. 2011), and spurs the creation of new start-ups and markets (Yeboah-Boateng and Essandoh 2014).

Table 2. Cloud threats prevalent in the literature

Category	Threats
Privacy and security	• Confidentiality of data hinders cloud (e.g. Chebrolu 2011; Kalyvas et al. 2013) • Sensitive data not suitable for cloud (e.g. Garrison et al. 2012; Noor et al. 2013) • Insider and outsider attacks (e.g. Dutta et al. 2013; Kim 2009) • Potential data loss (e.g. Armbrust et al. 2010; Kalyvas et al. 2013)
Compliance	• Regulations and integrity to laws (e.g. Kim 2009; Noor et al. 2013) • Location of data critical (e.g. Srinivasan 2013; Sultan 2011)
Integration	• Cultural resistance to change (e.g. Oredo and Njihia 2014) • Integrating new apps (e.g. Mather et al. 2009; Stanoevska-Slabeva and Wozniak 2010) • Unsuitability for migrating some existing applications (e.g. Oredo and Njihia 2014)
Reliability	• Availability of servers(e.g. Dutta et al. 2013; Voorsluys et al. 2011) • Offers from untrusted providers (e.g. Buyya et al. 2009; Kim 2009) • Congestion (e.g. Sultan 2011) • Unpredictability (e.g. Jaeger et al. 2008; Srinivasan 2013) • Bugs in large distributed systems (e.g. Armbrust et al. 2010; Kim 2009) • Downtime (e.g. Srinivasan 2013; Sultan 2011) • Poor broadband connectivity (e.g. Armbrust et al. 2010) • Data transfer bottlenecks (e.g. Armbrust et al. 2010)
Reversibility	• Contractual reversibility (e.g. Garrison et al. 2012; Sultan 2011) • Technical reversibility (e.g. Kalyvas et al. 2013)
Standardization	• Limited customization (e.g. Stanoevska-Slabeva and Wozniak 2010; Rajendran 2013) • Competitiveness affected (e.g. Oredo and Njihia 2014)
Skills	• Lack of competences and training (e.g. Dutta et al. 2013; Kim 2009) • Not understanding how to use cloud technologies (e.g. Rajendran 2013)
Non-transparency	• Hidden costs (e.g. Dutta et al. 2013; Srinivasan 2013)

Researchers are also beginning to discuss how cloud technology can lead to more organizational ***agility*** (Garrison et al. 2012; He 2011; Rajendran 2013). Some argue that, through cloud computing, processes can become more agile, departments work together and communicate more effectively (Yeboah-Boateng and Essandoh 2014), and IT-enabled projects have a lower time-to-market (Chebrolu 2011). Furthermore, cloud technology increases ***utilization*** of IT resources, both in terms of increasing end use (Marston et al. 2011) as well as by increasing the utilization of computing capacity through resource virtualization (Armbrust et al. 2010). Finally, Buyya et al. (2009), Onwubiko (2010) and Rajendran, (2013) state that the ***ubiquitous*** characteristics of cloud technology make it more attractive, since users can access their data anywhere they are, anytime they want, and via any device they have.

Table 2 summarizes the list of threats (or potential risks) found in the recent academic literature. Researchers most prominently cite ***privacy and security*** issues: storing sensitive and confidential data in cloud can be an important problem for organizations (Jaeger et al. 2008; Oredo and Njihia 2014; Voorsluys et al. 2011). Managers feel insecure due to possible insider and outsider cyberattacks (Srinivasan 2013; Sultan 2011). Therefore, organizations using cloud technology need to protect their data from being lost and from such attacks (Armbrust et al. 2010). Many researchers also argue that locating data in the cloud brings about ***compliance*** issues where data should abide by national and supranational laws and regulations such as the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), or the Cloud Service Level Agreement Standardization Guidelines issued by the EU Commission (Dutta et al. 2013; Jaeger et al. 2008; Srinivasan 2013). Organizations witness regulatory ambiguities when their data are located in another country and abide by the respective laws (Jaeger et al. 2008; Kim 2009).

Moreover, as cloud computing enters organizations as a new technology, researchers notice ***integration*** issues both referring to cultural resistance and to the technical transition of applications and processes to the cloud (Oredo and Njihia 2014), indicating that not all existing applications will be equally suitable for migration to the cloud. A larger number of authors mention that cloud services are ***standardized***, which limits the scope for organizations to differentiate from each other (Chebrolu 2011; Oredo and Njihia 2014; Rajendran 2013). Therefore, this lack of customization possibilities of cloud services, affects competitiveness, as noted by Oredo and Njihia (2014). Others argue that cloud computing is not really ***reliable*** (Sultan 2011; Voorsluys et al. 2011). These authors put forward that cloud servers are

unpredictable (Voorsluys et al. 2011), often unavailable (Kim 2009), and congested (Sultan 2011) with data transfer bottlenecks (Armbrust et al. 2010). Cloud computing is also susceptible to technical failures from bugs in large distributed systems as well as from poor broadband connectivity (Armbrust et al. 2010), both resulting in malfunction and downtimes (Srinivasan 2013). Kim (2009) notes that such failures are more likely when subscribing to solutions from untrusted providers.

According to Dutta et al. (2013), a vital issue when dealing with cloud technology is ***reversibility***, referring to both contractual and technical reversibility. Contractual reversibility consists in the lack of a reversibility clause in the signed contracts between users and the CSPs, which can lead to issues when users wish to retrieve their data or transfer them to another CSP (Dutta et al. 2013; Garrison et al. 2012; Oredo and Njihia 2014). Technical reversibility refers to vendor lock-in situations due to the lack of interoperability and data retrieval (Chebrolu 2011; Oredo and Njihia 2014; Voorsluys et al. 2011). Both forms of reversibility limit the freedom to switch from one CSP to another.

Lack of cloud-related ***skills*** was listed as a top issue in a recent survey of cloud computing challenges (Rightscale 2016). With the emergence of cloud technology, organizations require new expertise and competencies, and thus adequate trainings in order to understand the functionality of adopted cloud technology and underlying technologies (Rajendran 2013; Dutta et al. 2013; Oredo and Njihia 2014). Finally, some authors put forward that the cloud is not sufficiently ***transparent*** (Dutta et al., 2013; Srinivasan 2013), since there are hidden costs that users discover only at a later stage.

The maturing cloud computing literature covers both benefits and threats engendered by the adoption and use of cloud technology. However, our review provides that the cloud computing literature has not addressed these benefits and threats from the perspective of business and IT stakeholders in a firm. This we argue is an important gap, given that these two social groups need to resolve important governance and control conflicts related to the adoption and use of cloud technology (Winkler and Brown 2014; Khan et al. 2016).

Shadow IT

The shadow IT phenomenon has also been referred to in the literature as feral systems (Houghton and Kerr 2006), feral practices (Thatte et al. 2012), and un-enacted projects (Buchwald and Urbach 2012). These terms have in common that they describe the situation when business users acquire or use IT without required approval or oversight through corporate IT units. The emergence of shadow IT raises critical questions regarding its causes, its consequences, and required managerial coping strategies (Kopper and Westner 2016).

Commonly mentioned causes for shadow IT include unfulfilled needs and requirements of business departments and their dissatisfaction with the services provided by IT (Behrens and Sedera 2004; Jones et al. 2004; Boudreau and Robey 2005; Houghton and Kerr 2006; Huuskonen and Vakkari 2013; Kerr et al. 2007; Lyytinen and Newman 2015, Ahuja and Gallupe 2015). Some researchers add that shadow IT has emerged due to an increasing inflexibility, rigidity, and standardization of IT systems (Houghton and Kerr 2006). These characteristics inhibit IT departments from providing customized services fulfilling the totality of their business departments' needs.

Another potential cause is capability-based: Business users today develop their own competences in IT, which enables them to implement their own IT solutions (Behrens and Sedera 2004; Spierings 2012; Zimmermann and Rentrop 2014) especially if these acquired from external providers (Jones et al. 2004; Schalow et al. 2013; Ahuja and Gallupe 2015). The emergence of cloud computing has fueled the proliferation of shadow IT, since cloud technology often requires only a minimum IT competences from business users to customize and use them (Winkler and Brown 2014; Schalow et al. 2013). The literature has identified several other factors influencing the emergence of shadow IT in organizations, including business and IT misalignment (Zimmermann and Rentrop 2014), self-determination needs (Ahuja and Gallupe 2015), independency on IT department (Zainuddin 2012).

On the one hand, shadow IT is generally associated with a number of negative consequences. Most prominently, researchers cite unintended security and privacy issues (György et al. 2012; Schalow et al. 2013; Walters 2013; Kretzer and Maedche 2014; Walterbusch 2014): Organizations have witnessed how shadow IT can lead to non-compliance with organizational security policies (Alter 2014), data loss (Walters 2013), and disruption of controlled environments (György et al. 2012). Shadow IT can also cause a

loss of synergies between the different departments, as they are using solutions not provided by the IT department (György et al. 2012), and hence lead to the creation of resource conflicts between departments, having each of their own interests (Buchwald and Urbach 2012). It is important to highlight that employees may not be sensitized to the problems related to shadow IT, thus having a mindset that buying solutions from external (cloud) providers is not a risky task (Dittes et al. 2015).

On the other hand, the literature has also emphasized how the presence of some extent of shadow IT can have positive consequences for organizations. For instance, researchers have identified an increase in productivity as a positive effect when business departments short-cut their IT department (Ahuja and Gallupe 2015; Schalow et al. 2013). Using shadow solutions, where information is available at a glance, saves employees' time and helps them to focus on their job (Huuskonen and Vakkari 2013; Singh 2015). In addition to increased productivity, several researchers also mention increased business innovation as a positive effect (Behrens 2009; Singh 2015, Kretzer and Maedche 2014; Walterbusch 2014). Business innovation can, for example, be manifested in bringing organizational stability and order (Behrens 2009) or in helping personnel adapt to changes in their organizational environment (Singh 2015; György et al. 2012). Therefore, there is a duality where shadow IT can expose organizations to severe threats, while at the same time result in an improvement of organizations' business and IT capabilities.

Researchers have identified different managerial strategies to cope with this phenomenon. To prevent shadow IT, organizations set up governance structures and formal policies aiming at guiding employees across different levels (Walterbusch 2014; Zimmermann and Rentrop 2014) and creating awareness (Klesel et al. 2015; Walterbusch 2014). In order to better identify the unfulfilled needs of business departments, researchers advise organizations to integrate their business stakeholders in the IT decision-making process (Winkler and Brown 2014; Klesel et al. 2015). Organizations can start by identifying the different shadow IT systems through interviewing, interpreting help desk requests, and conducting technical analyses (Rentrop and Zimmermann 2012; Zimmermann et al. 2014; Walterbusch 2014). IT departments can conduct a network traffic analyses in order to monitor the evolution of shadow IT and identify systems with high dependency between business departments and external providers (Fürstenau and Rothe 2014).

While the shadow IT literature has provided important insights related to this phenomenon, we lack knowledge how these causes, consequences and managerial strategies map to the interpretation of business and IT stakeholders. This represents an important research gap since, according to technological frames, organizations would typically be interested in seeking a balance between these two different social groups.

Technological Frames Perspective

Technological frames as a theoretical perspective was coined by Bijker (1987) in his seminal work on how social contexts shape the design and use of technological artifacts using the historical examples of bikes, bakelites and bulbs. According to Bijker (1987), technological artifacts can be interpreted in rather flexible ways by different actor groups who often draw on their knowledge, experience, expectations, and interests; such interpretation flexibility and consequently differences in interpretations will then initiate interactions among these actor groups, which will in return influence the development of the technology itself. Later, this concept was introduced to the IS field by Orlikowski and Gash (1994), who conceptualized technological frames as a "subset of members' organizational frames that concern the assumptions, expectations, and knowledge they use to understand technology in organizations. This includes not only the nature and role of the technology itself, but the specific conditions, applications, and consequences of that technology in particular contexts" (p. 178). Technological frames emphasize how social context shapes individuals' interpretation of technology and also how such interpretations influence "technology development, implementation, and use" (Orlikowski and Gash 1994). Orlikowski and Gash (1994) have also identified four domains of technological frames, including frames related to features/attributes of the technology, frames related to development of technology, frames related to organizational application of the technology, and frames related to the organizational practices of the technology.

It is noted that individuals within a stakeholder group are likely to share a similar understanding of technology, which is referred to as "frame congruence," while "frame incongruence" might exist across groups (Davidson 2006; Orlikowski and Gash 1994). Such conceptualization of congruence/incongruence

has been drawn upon as the main tool by researchers adopting the technological frame perspective in attempts to understand the interpretive process and outcomes that are related to IT within organizations through comparing technological frames across one or more groups in the organization (e.g., Orlikowski and Gash 1994; McLoughlin et al. 2000; Lin and Cornford 2000; Lin and Silva 2005; Karsten and Laine 2007; Yeow and Sia 2008; Khoo and Hall 2013). The acknowledgement of the importance of frame congruence for the success of organizational IT activities also led a number of studies to examine the nature of interventions required to resolve incongruence, which often involved power and politics (e.g., McLoughlin et al. 2000; Lin and Conford 2000; Lin and Silva 2005; Young et al. 2016).

In this study, we apply technological frames to cloud technology, where we focus on two main actor groups that are closely involved in organizational adoption of cloud technologies: business and IT managers. Our goal is to analyze whether and how these two stakeholder groups perceive cloud technologies in different ways, given the differences in the knowledge, experience, expectations, and interests associated with these two groups respectively. We strive to analyze two domains of technological frames, following Mishra and Agarwal (2010), namely the benefits frame and the threat frame. The benefits frame represents the perception of the potential value added by cloud computing to organizations, whereas the treat frames represent the perception related to potential vulnerabilities and losses organizations might be exposed to when adopting cloud technologies (Mishra and Agarwal 2010). Such focus is also consistent with the outcome of our literature review, where existing studies have debated on the benefits/threat elements of cloud computing for organizations. Beyond these two categories, the technological frames perspective also encourages researchers to identify and develop novel frame categories and domains pertinent to the phenomenon of interest (Davidson 2006).

Methodology

In order to address our research question on the *technological frames that business and IT managers have regarding cloud computing*, we chose an interpretive approach based on qualitative data (Klein and Myers 1999). In the words of Orlikowski and Baroudi (1991), "interpretive studies assume people create and associate their own subjective and intersubjective meanings as they interact with the world around them." We attempt to understand cloud computing adoption and use through accessing the meanings business and IT managers attribute to this technology, rather than trying to find the objective 'truth' about it. We chose interviews as our primordial data source given that interviews enable researchers to examine different views and interpretations of individuals and groups (Walsham 1995). We would like to point out that the literature review will serve as the guidance for our data analysis. However, our goal is not to validate the benefits and the threats of cloud computing revealed by the literature review. Therefore, one can argue that our investigation employs elements of both deductive and inductive reasoning.

Data Collection

Our data is based on interviews with 10 business managers and 10 IT managers in large French organizations. We approached members of a professional association as well as selected alumni from the first author's university who had gained at least initial experience with one or multiple cloud services in their organizations. All participants were in IT management or business management roles, or external consultants reporting on their client organizations from a business perspective. Our focus on participants from large organizations was motivated by prior research that has provided evidence for cloud computing implementations being more challenging for larger organizations (Winkler et al. 2014; Venters and Whitley 2012). However, it should be noted that the unit of our analysis was not the organization, but the business managers and IT managers as social groups. Choosing individuals from different organizations allows us to abstract from the specifics of their organizational contexts and focus on the general differences between these two groups.

Table 3 displays details of the participants' roles, their companies' industries, as well as the cloud service models used by the company. All interviews were conducted in-person by the first author between December 2015 and April 2016 and lasted between 35 and 88 minutes (57 minutes on average). Our semi-structured interview guide contained 10 questions related to the participants' opinions about cloud computing (e.g., "what are your perceived benefits of cloud technology?", "what are your perceived threats?", "to which extent do business departments use cloud technology?", "Are there any issues?"). Business and IT managers received the same questions. All interviews were recorded with the consent of

Table 3. Interviewee characteristics

Ref.	Role	Industry	Adopted CC services	Ref.	Role	Industry	Adopted CC services
B1	CEO	Telecom	SaaS	IT1	CIO	Transportation	PaaS, SaaS
B2	CEO	Social security	SaaS	IT2	CIO	Social Security	PaaS, SaaS
B3	Sr. project mgr.	Health	IaaS, SaaS	IT3	Sr. IT mgr.	Research	IaaS, SaaS
B4	CEO	Web services	SaaS	IT4	CIO	State Security	PaaS, SaaS
B5	Mgmt. consultant	Entertainment	IaaS, PaaS, SaaS	IT5	CIO	Energy	IaaS, SaaS
B6	CEO	Telecom	SaaS	IT6	CIO	Energy	IaaS, SaaS
B7	CEO	Software	PaaS	IT7	CIO	State Security	SaaS
B8	Mgmt. consultant	Retail	IaaS, PaaS, SaaS	IT8	IT mgr.	Software	IaaS, SaaS
B9	CEO	Hospitality	SaaS	IT9	CIO	Bank	SaaS
B10	Mgmt. consultant	Transportation	IaaS, PaaS, SaaS	IT10	CIO	Retail	SaaS

the participants and subsequently transcribed. For the purpose of presentation in this paper, all quotations were translated from French into English.

Data Analysis

We used the software NVivo (version 11) to code our transcribed interviews. The analysis was guided by a critical, self-reflecting and skeptical perspective as suggested by Elliott and Timulak (2005). We started by dividing our data into distinctive meaning units; units communicating sufficient information for the reader even without the context (Elliott and Timulak 2005). In a first round of coding, we assigned the different fragments text to a set of emerging codes. We then used the categories gained from the literature review (i.e., the benefits and threat categories from Tables 1 and 2) as a coding scheme to which we assigned the codes from the first coding round, as suggested by Elliott and Timulak (2005). Coding samples can be found in the Appendix.

In this process, we also allowed additional categories to emerge from the data that did not fit the coding scheme. Here, we ultimately identified a new frame domain, which we termed as frames related to governance and control of shadow IT. This frame represents business and IT managers' perceptions of governance and control of cloud technologies, as we will elaborate below. To address our research question on stakeholder-specific views, we then contrasted quotations from business and IT managers and built three frames as displayed in Tables 4-6. For illustrative purposes, our analysis will also provide category-level code frequencies for business versus IT managers' view. Finally, we revisited the data to explore relationships between the benefits and threat frames on the one hand and governance and control frames on the other in the light of the technological frames perspective.

Findings

Benefits Frames

Table 4 illustrates the benefits frames held by the business and IT groups regarding cloud technology. Our results illustrate different benefit frames of cloud computing by the interviewed business and IT managers. While the business group particularly emphasizes the benefits generated by cloud technology (total frequency of 19), the IT managers group has less focus on benefits (freq. of 9). The benefits frame of the business group encompasses the *economics*, *agility*, *performance* and *ubiquity* aspects of cloud computing; the benefit frame of the IT group includes only *economic, agility* and *scalability* aspects.

Even though both business and IT groups invoke the ***economic*** benefits of cloud, there are nuanced differences in their understanding of these economic benefits. While business participants generally emphasize that the cloud is economically very attractive because "*large providers offer attractive solutions at super low prices"* (B8), a low price of these solutions is not mentioned by the IT participants. The IT managers emphasize more specific economic aspects including the pay-per-use characteristic of

Table 4. Findings: Benefits frames of business and IT managers				
	Business managers		**IT managers**	
	Category	Freq.	Category	Freq.
Benefits Frames	Economics • Low price of solutions (B1, B2, B3, B4, B5, B6, B8, B10)	8	Economic • Pay-per-use (IT5, IT7) • Variabilization of costs (IT1, IT6)	4
	Agility • Time-to-market (B2, B4)	2	Agility • Agile processes (IT1, IT5)	2
	Performance • Good quality of services (B1, B7, B8) • Improved productivity (B9,B10)	5	Scalability • Scaling up and down (IT4, IT6, IT8)	3
	Ubiquity • Ubiquitous access (B3, B5, B6, B10)	4		
	Total frequency	19	Total frequency	9

cloud computing, along with the variabilization of costs, where "*instead of buying huge hardware and material, [they] can choose the services that meet [their] needs*" (IT6).

Another benefits frame category shared by both groups is the ***agility*** generated by cloud technology. However, this benefit is also viewed from different angles, where the business group focuses on the shortened the time-to-market and the IT group focuses on the agile processes. For example, B4 explains how their business department quickly switched to a SaaS solution to "*finish a project in a very short period of time*" when no other resource was available. In comparison, IT1 states that cloud computing allowed the achievement of "*implemented continuous integration, continuous development, and DevOps*" (IT1). Hence, we notice that although business and IT participants agree on the agility benefits of cloud computing, this agility means different things for them.

In addition, there are specific aspects of cloud computing that are mentioned only by business or IT managers. The business managers particularly accentuate the ***performance*** benefits, where cloud technology provides good quality and "*no bugs so far, nor a downtime*" (B1). In addition, some business participants emphasize on the improved productivity when adopting cloud technology giving them, for example, "*a gain of one hour of productivity per day*" (B9). Moreover, some business participants express their satisfaction with the ***ubiquitous*** nature of cloud computing. Their quotes show the way cloud technology facilitates their work, rendering it easier for them to access their files and their data anywhere, anytime, anyway they want, "[They] like the fact that information are […] accessible via the Internet" (B3). On the side of the IT group, some participants refer to the ***scalability*** of cloud computing, which is especially important for applications "*dealing with a large number of users"* (IT4) and needing *"salability to easily increase capacities*" (IT4).

Threat Frames

Table 5 illustrates the threat frames held by the business and IT managers regarding cloud technology. From a quantitative point of view, it becomes obvious that the IT managers put more emphasis on the threats related to cloud computing (total freq. of 25) than the business managers (total freq. of 6).

Both groups focus on the ***security*** threats associated with cloud computing. For instance, the business and IT participants mention their fear of storing sensitive data in the public cloud, avoiding "*breaches and intrusion, which are one of [their] major concerns*" (B2). Similarly, the IT participants mention that they are "*particularly vigilant against any data leak*", which pushes them to avoid storing their employees' and clients' sensitive data in public cloud. In addition to data sensitivity, business stakeholders stress the presence of outside attacks threatening their organizations, and IT participants focus on the potential threats from losing their data. Data privacy is viewed as a very sensitive topic, especially when dealing with personal information. IT participants show low trust in cloud technology; they would not store their organizations' critical data in any third-party's datacenter to avoid losing them. For instance, IT1 explains the reasoning behind not storing critical data in a public cloud "*if the application stops working or if [their] files get lost then [they] face a serious issue with [their] employees, operations, and customers*." It is also important to notice that all 10 IT participants share the security threats from adopting cloud technology, where only 4 business participants were concerned about these threats.

Table 5. Findings: Threat frames of business and IT managers				
	Business managers		**IT managers**	
	Categories	Freq.	Categories	Freq.
Threat Frames	Security • Outside attacks (B2 • Data sensitivity (B4, B7, B9) Compliance • Location of data (B2) • Regulation and integrity laws (B9)	4 2	Security • Data loss (IT1, IT4, IT5, IT7, IT8, IT9) • Data sensitivity (IT2, IT3, IT6, IT10) Compliance • Location of data (IT4, IT5, IT9) • Regulation and integrity laws (IT3, IT6, IT7, IT10) Reversibility • Technical reversibility (IT2, IT5, IT8, IT10) • Contractual reversibility (IT6) Dependency • Dependency on suppliers (IT2, IT7, IT10)	10 7 5 3
	Total Frequency	6	Total Frequency	25

Compliance threats are a shared perception by both groups. Business and IT participants mention the data location threat generated by public cloud technology. For instance, organizations "*do not wish to put [their] data outside the Euro zone*" (B2), and are concerned by the location of their data in the cloud: "*[they] do not know where [their] data are hosted, or how to erase them, or where they appear when they are in the cloud*" (IT4). In addition, our participants express their concerns regarding the regulations and integrity laws that differ from one country to the other. An IT interviewee explains the situation that European organizations are put in: "*if [an organization was] on an international cloud and [their] CSP informs [them] that their servers are in the USA, it means that they abide the American laws*" (IT3). They then continue, "*This causes a data protection problem, meaning [their] CSP can put [their] data under the American justice if needed*" (IT3). Hence, there is a great awareness for the regulatory issues among the IT group.

Finally, while the IT participants also focus on the ***reversibility*** and ***dependency*** threats, the business participants do not mention other threats engendered by cloud technology. Technical and contractual reversibility are accentuated by some IT participants. They emphasize the role that the reversibility issue plays when adopting any new cloud solution, and they warn that "*going out of the cloud will be our nightmare in 10 years*" (IT5). They also argue that business managers do not see how critical this issue is. One remarks that due to the contractual reversibility of cloud technology, application software developed in the cloud is often "*not recoverable, since they are developed in particular languages and on different underlying platforms*" (IT6), making it impossible to switch from one CSP to the other. Another perceived cloud threat that was not pronounced in the literature review, but emerged from our analysis, is the dependency on the providers. The IT participants feel that organizations will become dependent on CSPs, who "*have their own visions and own objectives*" (IT3). CSPs having their large set of clients, can manipulate the organization by increasing the services prices, for example, making their clients extremely dependent on them.

Governance and Control Frames

Besides the benefit and threat frames, our inductive analysis also led us to conceptualize an emerging frame domain with quotations related the phenomenon of shadow IT, which we term as frames related to the governance and control of IT (Györy et al. 2012, Winkler and Brown 2014). Two sub-categories of this frame emerged that capture the participants' views: practicing governance through concrete action, and defining or re-defining governance through changes in the decision making structures of the organization. Table 6 displays abbreviations of key quotes from business and IT managers in these two sub-categories.

Business managers essentially perceive shadow IT as common business practice. All business participants acknowledge that their departments mostly "*buy software solutions from [cloud] providers*". Most participants do not feel that this is something unusual, although some are aware that this can be a problem: "*Well, shadow IT is a bit complicated to explain and to defend*" (B8). These business managers then refer to their specific needs, which directly link back to their benefits frames. One of these benefits is agility: "*The business departments are moving fast, with more work and short deadlines, due to the fast-moving market. So it is understandable that they get the solution the minute they need it*", IT8. Another benefit relates to performance: "*The communication department needed to store 50 Terabytes of video files […] and they searched for providers offering large storage capacities and a good quality*", B7.

Table 6. Governance and control frames of business and IT managers

	Business managers	**IT managers**
Frames related to practicing shadow IT	• General existence of shadow IT (B2) • Using local department budget for purchasing (cloud) software solutions (B3) • Local buying of cloud IT to enhance technical capabilities by solutions that internal IT does not provide (B7) • Circumventing IT department due to long provision times (B6) • Shadow IT to fulfill demands of more fast-moving business managers (B8)	• Shadow IT requires IT expertise (IT6) • Some shadow IT, generating security issues (IT5) • Business departments have no budgets for cloud IT (IT9)
Frames related to (re-) defining governance	• Business managers become more empowered through cloud; IT managers are not needed for software purchases (B1) • IT managers are no longer in control (B10) • IT managers are not able to keep up with the offers by the external market (B4) • Even proactive IT departments are not able to full specific needs (B5) • Making business departments aware of risks does not reduce shadow IT (B9)	• IT department controls everything related to IT (IT4) • Business departments need permission from IT departments (IT2). • Business department only has rights to acquire low-risk IT (IT10) • Business departments are not allowed contact cloud providers (IT7) • …and Cloud providers cannot approach business departments (IT1) • Shadow IT is not a problem because IT is responsive (IT3) • The open culture between business and IT renders shadow IT unnecessary (IT8)

In the eyes of IT managers, in contrast, shadow IT either does not occur ("*business departments do not buy solutions from cloud service providers*", IT9), or only at a very limited scale ("*we witness some shadow IT actions*", IT6). The IT stakeholders cite different reasons for why they see this phenomenon as rare, for example since "*business departments do not have the budget*", "*it is [the IT department] that controls IT*" (IT9), and "*our expertise is still required*" (IT6). Those who acknowledge the existence of shadow IT, heavily emphasize the risks, linking back to their threat frames. For example, IT5 emphasizes that "*shadow IT is really dangerous. Especially when business departments do not pay full attention to the CSP trustworthiness, the quality of their services, and particularly to the security issues*."

On the level of defining governance, business stakeholders essentially anticipate that the internal distribution of IT decisions-making power will need to be redefined in a way that business managers take stronger governance, and IT managers will lose control. Business managers "*feel [they] possess new powers through the cloud*" (B1) and that "*the IT department is no longer in total control of the organization*" (B10). As reasons for this perceived general development in which governance is shifting, they cite the lack of responsiveness of IT departments who are "*not able to fulfill all sorts of needs today*" (B4). Even an IT department that "*tries to take the initiatives and be proactive*" will, according to their view, not be able to fulfill their "*business departments' need [for] specific software*" (B5), which links back to their benefits frames of increased performance.

In the minds of IT managers, in contrast, their exertion of governance and control should be strengthened to prevent business managers from using cloud IT in the shadows. There is a strong mental liaison to the idea that "*the IT department controls anything related to IT*" (IT4) and that business "*departments need to get the [IT department's] permission before seeking solutions from cloud providers*" (IT2). Some are willing to grant business managers "*small budgets to buy software that is not harmful*" (IT10), but generally Business departments "*are not allowed to go behind and contact cloud providers on their own"* (IT7). Contrasting with the business view, IT stakeholders are convinced that responsiveness and a culture of being a "*more discussion-kind of organization*" (IT8) helps to address potential shadow IT issues: "*I don't think shadow IT is a huge problem in our organization, of our policies, stating that we build together with the business department, so if they need anything, we are here for them*" (IT3). In conclusion, there is a stark incongruence in how business and IT stakeholders have established their technological frames regarding the governance and control of cloud-based IT. In the views of business managers, shadow IT is a common business practice, which will question the 'raison d'être' (the reason of being) of corporate IT departments in the near future; in the minds of IT managers, shadow IT is only a small-scale issue, since the overall governance, the believe, is in most cases being defined in a way that

prevents business from practicing shadow IT. These stark frame incongruences raise the question on the *relationship* between the benefits and threat frames on the one hand, and governance and control frames on the other.

Relationships between Frames

Figure 1 summarizes the findings from this qualitative interpretive inquiry into the two different types of frames and illustrates how benefit/threat frames and frames regarding governance and control are related. We draw on the technological frames perspective and query again our empirical data to further explore this mutual relationship.

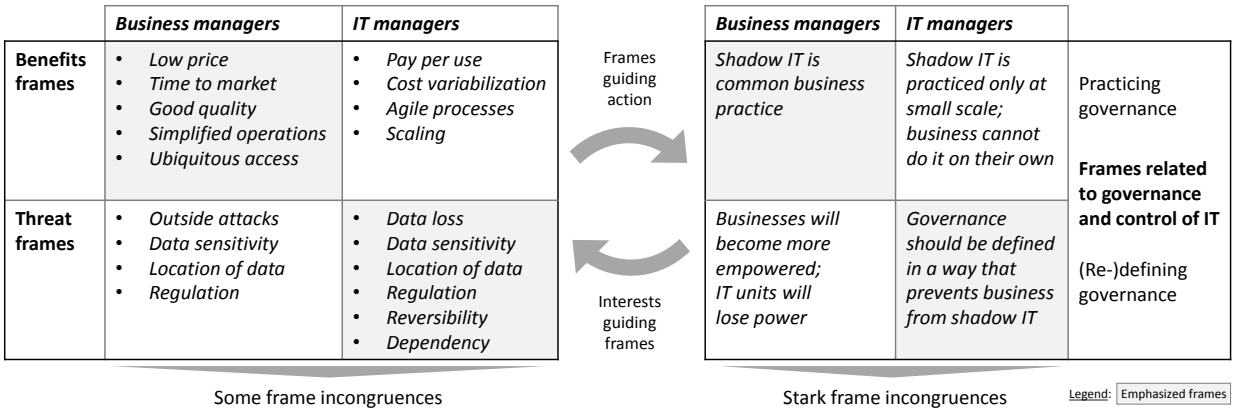

Figure 1. Summary: Frames of business and IT managers related to cloud computing

According to the technological frames perspective, different social groups form their perceptions of a certain technology according to their own background and interests (Orlikowski and Gash 1994), which are often situated within certain institutional context (Davidson and Pai 2004). When revisiting the data under this premise, we encountered additional quotes that highlight how the different interests of business versus IT managers shape their thinking about cloud computing benefits and threats. This thinking in turn guides their actions in existing organizational realities, as represented by the two circular arrows in Figure 1.

Statements by business managers revealed how the benefits of cloud technology speak to their own inherent interests such as business growth, competitive advantage, and innovation. One business interviewee, for example, states that their use of a SaaS CRM platform *"is helping the growth of [their] businesses as well as expanding [their] markets"* (B6). Business managers also wish to appear as early movers in the competition, which pushes them *"to implement the newest and most popular cloud solutions"* (B9). One business stakeholder believes that cloud technology has helped their organization become more innovative: "*We expect from the cloud a set of services that is going to allow developing new digital services*" (B5).

IT managers, as a social group, have very different inherent interests. Our empirical material suggests that their primary interests are to retain their jobs, their work processes, and their power in the age of cloud computing. IT managers expressed a concrete fear of becoming obsolete, asking themselves whether *"what I've been doing for the past 10 years is useless now?"* (IT9). They feel offended if other departments bypass IT by using cloud technology and they have difficulties to adapt to new cloud-based delivery models: *"human resistance is strong regarding changes in our internal processes"* (IT1). They also fear losing their power within the organization: *"In the last couple of years, business departments started buying SaaS solutions from CSPs when they noticed that our IT department didn't have the required reactivity or agility to fill their needs. Allowing our business departments to get SaaS solutions from CSPs means our IT department needs to pass the 'decision hand' to the business departments; but we will not allow this due to internal and external political reasons"* (IT10). Thus, retaining the power

within IT organizations plays an important role IT stakeholders, as they do want give away power to business departments or other external parties in the cloud ecosystem.

Hence, these quotes indicate how benefits and threats frames on the one hand, and governance and control frames on the other, are mutually related: One the one side, business manager's desire for business growth and innovation may lead them to (over-)emphasize the benefits frames and therefore practice governance, i.e. shadow IT, without invoking potential threat frames. This is exemplified by the following quote: "*[We] possess new powers through the cloud, and specifically through shadow IT, where [they] do not really need the IT department to get software*" (B1).

On the other side, the inherent fear to lose governance and control may blind IT stakeholders of the existence of shadow IT, and to (over-)emphasize the threat frames regarding cloud computing. This emphasis of the threat frames, from a technological frames perspective, can be seen as an intent to reframe the understandings and expectations of the other social group with the goal to establish congruence (Orlikowski and Gash 1994; Davidson and Pai 2004; Davidson 2006). That is, IT stakeholders may to some extent use threat frames as a pretext to influence business stakeholders towards a more restrictive use of cloud service, with the goal to mark and retain their traditional territory. In fact, one IT interviewee admits: "*We are at the end of an era where internal IT operations were the domain of IT people, considering themselves the only ones with the appropriate skills to deal with such operations. There is obviously a strong psychological liaison to this idea in IT departments. This is why we invented this 'security story', to justify the fact that we are moving slower*" (IT8).

Discussion

Motivated by the current lack of stakeholder-specific research inquiries in the cloud computing literature, this study set out to explore the differences of business managers and IT managers' technological frames related to cloud computing. Our findings, first of all, indicate that business managers primarily emphasize the benefits frames, stating that implementing cloud technology can lead to *economic* benefits, increased *performance*, more business *agility*, and more *ubiquitous* access to data. In contrast, IT managers primarily stress the threat frames, stating that these solutions can lead to *security*, *compliance*, and *reversibility* issues where companies become *dependent* on the cloud service providers. Beyond these differences in the intensity to which specific frames are emphasized, we also found nuanced qualitative differences within some of the shared categories: While business managers think of economic benefits in terms of cost saving, IT managers qualify economic benefits as the pay-per-use characteristics of cloud and the variabilization of costs; while business managers associate *agility* with increased time-to-market, IT managers think more about the agility of IT delivery processes.

While being descriptive in nature, these nuanced differences in intensity and interpretation of the benefit frames through these two stakeholder groups represent a novel contribution to the cloud adoption literature (e.g., Buyya et al. 2009; Chebrolu 2011; Benlian and Hess 2011; Dutta et al. 2013). As our initial review provides (Tables 1-2), this literature has comprehensively covered different categories of benefits and threats, which the individual frames of the two stakeholder groups can be related to and are consistent with. To the best of our knowledge, however, none of the prior cloud computing studies has addressed the stakeholder-specific interpretations of these benefits and threats. Hence, our stakeholder-specific, interpretive look at benefits and threats is an important contribution to the literature on cloud adoption as it shows that specific cloud adoption rationales are not necessarily invoked equally across some studies stakeholder groups. In other words, our findings add to the widely cited and seemingly understood benefits and threats of cloud computing (e.g., the commonly cited performance versus security tradeoffs of cloud computing) an important interpretive nuance, suggesting that some of these aspects may be up-played or downplayed depending on the social groups that are involved.

Second, our analysis spawned a third category of frames regarding the *governance and control of (cloud) IT*. Two sub-categories of emerged from our data referring to practicing governance versus defining governance. Our findings highlight how business and IT stakeholders construe very different stories of how governance and control of cloud IT is being exerted, and how it should be defined (Table 6): Business managers see shadow adoption of cloud IT as a common business practices which questions the raison d'être of corporate IT department in the near future; IT managers mostly view shadow IT as a small scale

issue and trust in the overall IT governance that would prevent the company from major shadow IT issues.

We analyzed the mutual relationships between benefits/threats on the one hand and governance and control on the other and explain the frame incongruences in the light of technological frames perspective as being the result of fundamentally different underlying interests: While business managers views are shaped by the wish to use cloud technology as a means to achieve business growth, competitive advantage, and innovation, IT managers primary concerns with regard to cloud technology is to retain their jobs, work processes, and power in organizational realities. Following this line of thought, it only seems logical that business managers primarily invoke benefits frames and practice shadow IT, while IT manages primarily emphasize the threats and call for stricter IT governance and control.

Our findings therefore also contribute to the literature on shadow IT as they help us understand the duality around the often quoted shadow IT phenomenon. The emerging shadow IT literature has always emphasized two sides: shadow IT being a threat for corporate IT security (e.g., Behrens 2009; Walters 2013) versus a benefit in terms of business productivity and innovation (e.g., Györy et al. 2012; Jones et al. 2004). Our stakeholder-specific approach not only suggests that each of these sides, by and large, maps to one of the two stakeholder groups, but it also provides an interests-based explanation for why this is the case: Business productivity and innovation benefits through shadow IT are primarily emphasized by business managers, because it is their inherent interest to pursue these business goals; corporate IT security threats are primarily stressed by IT managers, since it is in their very own interest not only to ensure corporate IT security goals, but also to retain their role and power in organizational realities.—The prior shadow IT literature has lacked explicit consideration of contrasting business and IT stakeholder views (Kopper and Westner 2016). Our results indicate that studies of shadow IT perceptions are strongly subject to who are participating subjects. Future shadow IT research should therefore be aware of these perceptual biases when defining the research design for studies that address the shadow IT phenomenon.

Theoretical Implications

Besides contributing to the emerging cloud computing and shadow IT literatures, we believe this study also holds three theoretical implications for the use of the technological frames perspective.

First, we applied the concept of technological frames to a broader technological trend and service delivery model innovation, which generated new insights. Compared with existing literature on technological frames (e.g., Davidson 2006; Lin and Silva 2005; Orlikowski and Gash 1994; Young et al. 2016), the novel technological context—that of cloud computing—has revealed different dynamics when it comes to congruence/incongruence of technological frames between various stakeholder groups. More specifically, the nature of incongruences between the business managers and the IT managers we have witnessed in the case of cloud computing is no longer centered on frames related to features or attributes of the technology, frames related to development of the technology, and frames related to the organizational application of the technology—which are the main frame domains observed in existing literature (Davidson 2006). Instead, the focal conflict between these two stakeholder groups regards frames related to organizational practices of the technology, and more specifically frames related to the governance and control of this technology. We argue that such results can be attributed to the fact that the nature of the cloud technology differs to that of traditional on premise solutions. In the case of cloud computing, user organizations are liberated from much of the responsibilities associated with setting up and maintaining the solutions (this is especially the case with SaaS), which traditionally used to be handled in-house by the IT unit in the on-premise scenario (Martinson et al. 2011, Winkler and Brown 2014). In other words, the business unit and the IT unit no longer struggle (or struggle much less) to be aligned on these issues, as cloud computing has enabled the business unit to choose and set up the solution that fits their bill without much involvement from the IT department. Therefore, from a theoretical point of view, this study demonstrates how a certain technological context influences the nature of frame congruence/ incongruence associated with such technology.

Second, researchers have called for focusing more on the structure, domains, and relationship of the frames themselves (Davidson 2006; Mishra and Agarwal 2010). Our exploratory analysis started deductively from a two-part structure of benefits and threat frames adopted from prior studies (Mishra and Agarwal 2010), and then spawned an additional domain during the inductive analysis of the data. We labelled this emerging domain as *frames related to governance and control of the technology*, referring

to knowledge and expectations about the distribution of decision rights (Winkler and Brown 2014), which guide actor's in their interpretations and actions. While this novel domain can be seen as similar to Orlikowski and Gash's (1994) more generic domain about *frames related to incorporating IT to work practices*, the governance and control domain refers specifically to the decision making about (and not to the use of) a technology. As argued initially, the increasing proliferation of information technology within and across organizations may justify considering governance and control as a frames domain that stands for itself, when exploring the meaning that groups attach to these emerging technologies. Furthermore, we argue that it would take much more than communication to align the technological frames related to governance and control of the technology, especially in the cloud context. This is because it involves rethinking and restructuring of roles and responsibilities of the business unit and the IT unit when it comes to IT deployment (Willcocks et al. 2014).

Third, while the technological frames perspective has mostly been used to explain relationships between frames and outcomes such as technology use, our discussion explored the relationship between frames of different domains, here specifically the relationship between benefits and threat frames one the one hand and governance and control frames on the other. Other researchers may find it helpful to reason about how (in-)congruences in one set of frames can translate into (in-)congruences in another. For example, as seen in our case of frames related to cloud technology, constituents may have diverging, but not fundamentally different perceptions in some frames (e.g., benefits and threats), which then translate into stark contrasts in another domain (e.g., governance and control). Worth noting, however, is that this relationship is not a straightforward one in that different domains of frames can clearly influence each other mutually.

Implications for Practice

Organizations that seek to adopt cloud technology should be aware of, and counteract these frame incongruences by resolving the underlying conflicts of interests between the involved stakeholders. Organizations need to effectively address the fears and concerns of their employees in IT. This can be achieved, for example, through adequate human resources actions such as developing new career paths and offering trainings that prepare IT employees in traditional roles for the management and use of cloud software, platforms, and infrastructure services, as also indicated by previous authors (Dutta et al. 2013 and Rajendran 2013). In addition, effective communication between stakeholders about benefits and threats of cloud technology may help to reduce incongruences of business and IT stakeholders' mindsets, and thus to 'lighten up' the shadows in which cloud IT is frequently run today (Walters 2013).

Limitations and Future Work

The limitations of this study point to future research opportunities in the field of cloud computing and shadow IT: First, given our focus on different social groups as unit of analysis, this qualitative study used respondents from different companies. Given this group focus, we were not able to assess to which extent the presence of incongruences led to negative consequences in a specific case. Second, we acknowledge that our data collection approach was limited by addressing members of one professional association and a university alumni network. Third, it is worth pointing out that our analysis was not sensitive to the different cloud service models (SaaS, PaaS, and IaaS) given that participants mostly referred to cloud technology collectively (though with an implicit focus on SaaS). Fourth, our study context of France should be considered when generalizing to other geographical contexts due to possible cultural, managerial, or legal variations.

Future researchers may want to adopt an organization-level focus to study technological frames related to different levels of cloud computing services in depth and include adequate outcome measures in this investigation. Particularly interesting also appears to be research that is designed to test the proposed relationships between frames, stakeholder interests, and shadow IT occurrence among a larger sample of organizations. The domains of cloud computing-related frames identified by this study and their proposed relationships may provide a solid ground for future research to build on.

Conclusions

In this study, we examined the organizational adoption of cloud computing by focusing on two stakeholder groups: business managers and IT managers. Drawing on a technological frames perspective, we compared and contrasted the knowledge and expectations that business versus IT managers have regarding cloud IT through a series of interviews with these stakeholders. Our analysis revealed the incongruences between these two groups' technological frames and how this relates to their governing actions: while business managers emphasize the benefits frames of cloud computing and tend to undermine IT governance, IT managers stress its threat frames and their desire to strengthen the IT governing framework. We then engaged in a discussion on how these frame incongruences are related and how they can be resolved. We believe this work contributes to both, the literature on cloud adoption and the shadow IT literature, by providing a stakeholder-specific view that helps understand, and in parts explain, the duality of the shadow IT phenomenon. From a theoretical point of view, we argue that our application of the technological frames lens has enabled us 1) to demonstrate how a certain technological context (i.e., cloud computing) influences the nature and dynamics of technological frames between different stakeholder groups; 2) to identify a new frame domain—frames related to governance and control of the technology—that is of specific importance to todays' proliferating information technology landscapes; and 3) to demonstrate how incongruences in one set of frames can translate into incongruences in another frame. Practically, our results offer advice to organizations that struggle with pre- or post-adoption issues related to cloud deployment by emphasizing the need for adequate human resources actions and communication approaches.

References

Ahuja, S., and Gallupe, B. 2015. "A Foundation for the Study of Personal Cloud Computing in Organizations," *Americas Conference on Information Systems (AMCIS) Proceedings*.

Alter, S. 2014. "Theory of Workarounds," *Communications of the ACM*, (34:1), pp. 1041–1066.

Andriole, S. J. 2015. "Who owns IT?," *Communications of the ACM*, (*58*:3), pp. 50-57.

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. 2010. "A view of cloud computing." *Communications of the ACM,* (53:4), pp. 50–58.

Behrens, S. 2009. "Shadow systems: The good, the bad and the ugly," *Communications of the ACM*, (*52:*2), pp. 124-129.

Behrens, S., and Sedera, W. 2004. "Why do shadow systems exist after an ERP implementation? Lessons from a case study," *Pacific Asia Conference on Information Systems (PACIS) Proceedings*.

Benlian, A., and Hess, T. 2011. "Opportunities and risks of software-as-a-service: Findings from a survey of IT executives," *Decision Support Systems*, (52:1), pp. 232–246.

Bijker, W. 1987. "The social construction of Bakelite: Toward a theory of invention," *The social construction of technological systems*, pp. 159-187.

Boudreau, M., and Robey, D. 2005. "Enacting integrated information technology: A human agency perspective," *Organization science*, (16:1), pp. 3–18.

Brynjolfsson, E., Hofmann, P., and Jordan, J. 2010. "Cloud computing and electricity: beyond the utility model," *Communications of the ACM*, (53:5).

Buchwald A, Urbach N. 2012. "Exploring the Role of Un-Enacted Projects in IT Project Portfolio Management," *International Conference on Information Systems (ICIS) Proceedings*.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., and Brandic, I. 2009. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, (25:6), pp. 599–616.

Chebrolu, S. B. 2011. "Assessing the relationships among cloud adoption, strategic alignment and IT effectiveness," *Journal of Information Technology Management*, (22:2), pp. 13–29.

Davidson, E. 2006. "A technological frames perspective on information technology and organizational change," *The Journal of Applied Behavioral Science*, (*42*:1), pp. 23-39.

Davidson, E. and Pai, D. 2004. "Making sense of technological frames: Promise, progress, and potential," *Information Systems Research*, pp. 473-491.

Dittes, S., Urbach, N., Ahlemann, F., Smolnik, S., and Müller, T. 2015. "Why don't you stick to them? Understanding factors influencing and counter-measures to combat deviant behavior towards organizational IT standards," *Multikonferenz Wirtschaftsinformatik Proceedings*, pp. 615-629.

Dutta, A., Peng, G. C. A., and Choudhary, A. 2013. "Risks in enterprise cloud computing: the perspective of IT experts," *Journal of Computer Information Systems*, (53:4), pp. 39–48.

Elliott, R. and Timulak, L. 2005. *Descriptive and interpretive approaches to qualitative research,* Handbook of Resolved Methods for Clinical and Health Psychology, pp. 147–159.

Fürstenau, D., Rothe, H. 2014. "Shadow IT Systems: Discerning the Good and the Evil,"*European Conference on Information Systems (ECIS) Proceeding*.

Garrison, G., Kim, S., and Wakefield, R. 2012. "Success factors for deploying cloud computing," *Communications of the ACM,* (55:9), pp. 62–68.

Gartner. 2016. "*Gartner Says By 2020, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today*." Retrieved from: http://www.gartner.com/newsroom/id/3354117 (visited on 24/03/2017)

Goundar, S. 2010. "Cloud computing: Opportunities and issues for developing countries," *DiploFoundation: Internet governance research paper*.

Györy, A. A. B., Cleven, A., Uebernickel, F., and Brenner, W. 2012. "Exploring the shadows: IT governance approaches to user-driven innovation," *European Conference on Information Systems (ECIS) Proceedings*.

He, Y. 2011. "The lifecycle process model for cloud governance," PhD Dissertation, University of Twente.

Houghton, L., and Kerr, D. V. 2006. "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 and Enterprise Management*, (4:2), pp. 135–147.

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

ITA. 2016. "*2016 Top Markets Report Cloud Computing: A Market Assessment Tool for U.S Exporters,"* Market Report 2016-05 U.S Department of Commerce, International Trade Administration. Retrieved from: http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf (visited on: 04/04/2017)

Jaeger, P., Lin, J. and Grimes, J. 2008. "Cloud Computing and Information Policy: Computing in a Policy Cloud?" *Journal of Information Technology & Politics,* (5:3), pp. 269–283.

Joha, A., and Janssen, M. 2012. "Transformation to Cloud Services Sourcing: Required IT Governance Capabilities," *ICST Transactions on e-Business*, (9:1).

Jones, D., Behrens, S., Jamieson, K., and Tansley, E. 2004. "The rise and fall of a shadow system: Lessons for enterprise system implementation," *Asian Conference on Information Systems Proceedings*.

Kalyvas, J. R., Overly, M. R., and Karlyn, M. A. 2013. "Cloud computing: A practical framework for managing cloud computing risk-part II," *Intellectual Property & Technology Law Journal*, (25:4), p. 19.

Karsten, H., and Laine, A. 2007. "User interpretations of future information system use: a snapshot with technological frames," *International journal of medical informatics*, *76*, pp. 136-140.

Khan, S., Nicho, M., and Takruri, H. 2016. "IT controls in the public cloud: Success factors for allocation of roles and responsibilities," *Journal of Information Technology Case and Application Research*, (18:3), pp. 155-180.

Khoo, M., and Hall, C. 2013. "Managing metadata: Networks of practice, technological frames, and metadata work in a digital library," *Information and organization*, (*23:*2), pp. 81-106.

Kim, W. 2009. "Cloud computing: Today and tomorrow.," *Journal of object technology*, (8:1), pp. 65–72.

Klein, H. K., and Myers, M. D. 1999. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," *MIS Quarterly*, (23:1).

Klesel, M., Mokosch, G., and Niehaves, B. 2015. "Putting Flesh on the Duality of Structure: The Case of IT Consumerization," *Americas Conference on Information Systems (AMCIS) Proceedings*.

Kopper, A., and Westner, M. 2016. "Deriving a Framework for Causes, Consequences, and Governance of Shadow IT from Literature," *Multikonferenz Wirtschaftsinformatik Proceedings*.

Kretzer, M., and Maedche, A. 2014. "Generativity of Business Intelligence Platforms: A Research Agenda Guided by Lessons from Shadow IT", *Multikonferenz Wirtschaftsinformatik Proceedings*, pp. 207-220.

Kundra, V. 2011. "Federal cloud computing strategy," Washington D.C: The White House.

Lin, A., and Cornford, T. 2000. *Socio-technical perspectives on emergence phenomena*, The New Sociotech: Graffiti on the Long Wall, E. Coakes, R. Lloyd Jones and D. Willis (eds.), London: Springer-Verlag.

Lin, A., and Silva, L. 2005. "The social and political construction of technological frames," *European Journal of Information Systems*, (14:1), pp. 49–59.
Lyytinen, K., and Newman, M. 2015. "A tale of two coalitions–marginalising the users while successfully implementing an enterprise resource planning system," *Information Systems Journal*, (*25:*2), pp. 71-101.
Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. 2011. "Cloud computing — The business perspective," *Decision Support Systems*, (51:1), pp. 176–189.
Mather, T., Kumaraswamy, S., and Latif, S. 2009. *Cloud security and privacy: an enterprise perspective on risks and compliance*, CA: O'Reilly Media Inc.
McLoughlin, I., Badham, R., and Couchman, P. 2000. "Rethinking political process in technological change: socio-technical configurations and frames," *Technology Analysis & Strategic Management*, (*12:*1), pp. 17-37.
Mishra, A. N., and Agarwal, R. 2010. "Technological Frames, Organizational Capabilities, and IT Use: An Empirical Investigation of Electronic Procurement," *Information Systems Research*, (21:2), pp. 249–270.
Noor, T., Sheng, Q., Zeadally S., and Yu J. 2013. "Trust management of services in cloud environments: Obstacles and solutions." *ACM Computing Surveys,* (46:1), pp. 12–47.
Onwubiko, C. 2010. "Security Issues to Cloud Computing," in *Cloud Computing*, N. Antonopoulos and L. Gillam (eds.), London: Springer London, pp. 271–288.
Oredo, J. O., and Njihia, J. 2014. "Challenges of cloud computing in business: Towards new organizational competencies," *International Journal of Business and Social Science*, (5:3).
Orlikowski, W. and Baroudi. 1991. "Studying information technology in organizations: Research approaches and assumptions." *Information Systems Research,* (2:1), pp. 1–28.
Orlikowski, W. 1996. "Improvising organizational transformation over time: A situated change perspective," *Information systems research*, (*7:*1), pp. 63-92.
Orlikowski, W. J., and Gash, D. C. 1994. "Technological Frames: Making Sense of Information Technology in Organizations," *ACM Transactions on Information Systems,* (12:2), pp. 174–207.
Pinch, T. J., and Bijker, W. E. 1984. "The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other," *Social studies of science*, (14:3), pp. 399–441.
Rajendran, S. 2013. "Organizational challenges in cloud adoption and enablers of cloud transition program," PhD Dissertation, USA: Massachusetts Institute of Technology.
Rentrop, C., and Zimmermann, S. 2012. "Shadow IT," *Management and Control of Unofficial IT. ICDS*, pp. 98–102.
Rightscale (2016). "*State of the Cloud Report – Hybrid Cloud Adoption Ramps as Cloud Users and Cloud Providers Mature.*" Retrieved from: https://assets.rightscale.com/uploads/pdfs/RightScale-2016-State-of-the-Cloud-Report.pdf (visited on 03/05/2017).
Schalow, P. R., Winkler, T. J., Repschlaeger, J., and Zarnekow, R. 2013. "The Blurring Boundaries Of Work-Related And Personal Media Use: A Grounded Theory Study On The Employee's Perspective," *European Conference on Information Systems*.
Singh, H. 2015. "Emergence and Consequences of Drift in Organizational Information Systems," *Pacific Asia Conference on Information Systems Proceedings*.
Spierings, A., Kerr, D., and Houghton, L. 2014. "What Drives the End User to Build a Feral Information System?" *Feral Information Systems Development: Managerial Implications*, pp. 161-188.
Srinivasan, S. 2013. "Is security realistic in cloud computing?," *Journal of International Technology and Information Management*, (22:4).
Stanoevska-Slabeva, K., and Wozniak T. 2010. *Cloud basics–an introduction to cloud computing*. Chapter in *Grid and cloud computing,* Berlin: Springer Heidelberg.
Sultan, N. A. 2011. "Reaching for the 'cloud': How SMEs can manage," *International Journal of Information Management*, (31:3), pp. 272–278.
Thatte, S., Grainger, N., and McKay, J. 2012. "Feral practices," *Australasian Conference on Information Systems (ACIS) Proceedings*, pp. 1–10.
Tiers, G., Mourmant, G., and Leclercq-Vandelannoitte, A. 2014. "Cloud Computing: les composantes d'une rupture".
Venters, W., and Whitley, E. 2012. "A critical review of cloud computing: researching desires and realities," *Journal of Information Technology,* (27:3), pp. 179-197.

Vishwakarma, A. K. 2012. "Cloud Computing: Future Generation Computing Systemsas the 5th Utility," *International Journal of Information and Electronics Engineering*, (2:2), p. 193.

Voorsluys, W., Broberg, J. and Buyya, R. 2011. *Introduction to cloud computing*. Chapter in *Cloud Computing Principals and Paradigms*, UK: John Wiley & Sons Press.

Walsham, G. 1995. "Interpretive case studies in IS research: nature and method." *European Journal of Information Systems,* (4:2), pp. 74-81.

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

Walters, R. 2013. "Bringing IT out of the shadows," *Network Security*, (2013:4), pp. 5–11.

Webster, J., and Watson, R. T. 2002. "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quarterly*, pp. xiii–xxiii.

Wei, J., Zhang, X., Ammons, G., Bala, V., and Ning, P. 2009. "Managing security of virtual machine images in a cloud environment," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 91–96.

Weick, K. 1979. *The Social Psychology of Organizing,* USA: McGraw-Hill, 2nd edition.

Winkler, T. J., and Brown, C. V. 2014. "Horizontal Allocation of Decision Rights for On-Premise Applications and Software-as-a-Service," *Journal of Management Information Systems*, (30:3), pp. 13–48.

Winkler, T. J., Benlian, A., Piper, M., and Hirsch, H. 2014. "Bayer HealthCare Delivers a Dose of Reality for Cloud Payoff Mantras in Multinationals," *MIS Quarterly Executives*, (13:4).

Yeboah-Boateng, E. O., and Essandoh, K. A. 2014. "Factors influencing the adoption of cloud computing by small and medium enterprises in developing economies," *International Journal of Emerging Science and Engineering*, (2:4), pp. 13–20.

Yeow, A., and Sia, S. 2008. "Negotiating "best practices" in package software implementation," *Information and Organization*, (*18*:1), pp. 1-28.

Young, B., Mathiassen, L., and Davidson, E. 2016. "Inconsistent and Incongruent Frames During IT-enabled Change: An Action Research Study into Sales Process Innovation," *Journal of the Association for Information Systems,* (17:1).

Zainuddin, E. 2012. "Secretly Saas-Ing: Stealth Adoption of Software-as-a-Service from the Embeddedness Perspective," *International Conference on Information Systems Proceedings*.

Zhang, Q., Cheng, L., and Boutaba, R. 2010. "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications*, (1:1), pp. 7–18.

Zimmermann, S., and Rentrop, C. 2014. "On the Emergence of Shadow IT: A Transaction Cost-Based Approach," *European Conference on Information Systems Proceedings*.

Zimmermann, S., Rentrop, C., and Felden, C. 2014. "Managing Shadow IT Instances: A Method to Control Autonomous IT Solutions in the Business Departments," *Americas Conference on Information Systems Proceedings*.

Appendix

Quotations	Codes	Sub-Codes
"Today, large providers are offering attractive solutions at super low prices. You cannot just disregard such offers and continue working with current expensive on-premises applications and machines." (B8)	**Economics**	*Low price of solutions*
"If our HR department needs a specific solution for some project, yes I would say that the cloud is beneficial because of the low solutions prices and the pay-as-you-go characteristic of the cloud." (IT5)		*Pay-per-use*
"Another reason [they] adopt cloud solutions is the price. Instead of buying huge hardware and material, [they] can choose the solutions that meet [their] needs and consult the different offers along with the level of security of these offers." (IT6)		*Variabilization of costs*
"We were skeptical about using cloud solutions, especially SaaS solutions, but I am so glad we did, because the CSP we are buying our SaaS solutions from, has an excellent quality of services which have not got bugs so far, nor a downtime." (B1)	**Performance**	*Good quality of services*
"This cloud service allowed us a gain of one hour of productivity per day, where cleaning ladies don't have to go call the head chief once they get to the room and once they finish cleaning it, but just check in with this application." (B9)		*Improved productivity*
"The government needs the cloud because of its high scalability and flexibility. We are dealing with a large number of users, where we cannot always forecast the flow and hence we need this ability to easily increase our capacities." (IT4)	**Scalability**	*Scaling up and down*
"We needed to adopt SaaS solutions [for Project Management] because we were given a very short time to finish this project that we had no other choice than to rely on cloud solutions." (B4)	**Agility**	*Time-to-market*
"As we are moving to more agility, we implemented continuous integration, continuous development, and DevOps. We noticed that the cloud facilitates our next steps to reach more agility." (IT1)		*Agile processes*
"[They] like the fact that information and processes are not local but are diffused throughout the network and accessible via the Internet." (B3)	**Ubiquity**	*Ubiquitous access*
"[They] cannot allow having intrusions to our systems. So security of the cloud is one of our major concerns." (B2)	**Security**	*Outside attacks*
"[They] were going to use the Google cloud platform and some google SaaS solutions, but when we found out that Google granted the American government access to the hosted data, it scared us and made us restudy our decision." (B7)		*Data Sensitivity*
"Being one of the largest transportation companies in France, [they] do not put critical applications on the cloud, because critical means that if the application stops working or if [their] files get lost then [they] face a serious issue with [their] employees, operations, and customers." (IT1)		*Data Loss*
"Our core business data are sensitive, so [they] do not wish to put [their] data outside the Euro Zone due to the numerous laws that other countries abide to." (B2)	**Compliance**	*Location of data*
"If you were in the USA you can do things that you cannot do if you were in France. Another issue would be, if you were on an international cloud and your CSP informs you that their servers are in the USA, it means that they abide the American laws. This causes a data protection problem, meaning your CSP can put your data under the American justice if needed." (IT3)		*Regulations and integrity to laws*
"Going out of the cloud will be our nightmare in 10 years. The day where we fight with our CSP or they become extremely expensive or we cannot agree on common grounds, it will be extremely harmful." (IT5)	**Reversibility**	*Technical reversibility*
"Our salesforces applications are applications made on salesforce.com. Thus their reversibility is quasi-impossible. Where do we put them afterwards? We can eventually recover our data but application software are not recoverable since they were developed in particular languages." (IT6)		*Contractual reversibility*
"If my contract ends and I cannot use the same CSP, how do I guarantee the continuity of the service? If the CSP changes rules, how do I deal with that?" (IT7)	**Dependency**	*Dependency on Suppliers*