5-15-2012

EXPLORING THE SHADOWS: IT GOVERNANCE APPROACHES TO USER-DRIVEN INNOVATION

Andreas Györy
University of St.Gallen

Anne Cleven
A² Research

Falk Uebernickel
University of St.Gallen

Walter Brenner
University of St.Gallen

EXPLORING THE SHADOWS: IT GOVERNANCE APPROACHES TO USER-DRIVEN INNOVATION

Andreas Göry, University of St.Gallen, Mueller-Friedberg-Str. 8, 9000 St.Gallen, Switzerland, andreas.gyoery@unisg.ch

Anne Cleven, A² Research, St.Jakob-Str. 93, 9000 St.Gallen, Switzerland, anne.cleven@unisg.ch

Falk Uebernickel, University of St.Gallen, Mueller-Friedberg-Str. 8, 9000 St.Gallen, Switzerland, falk.uebernickel@unisg.ch

Walter Brenner, University of St.Gallen, Mueller-Friedberg-Str. 8, 9000 St.Gallen, Switzerland, walter.brenner@unisg.ch

Abstract

Information Systems (IS) researchers traditionally have the assumption that Information Technology (IT) innovations are conceived within the IT department. Developments like ubiquitous computing, web services and the emerging culture of digital natives (DN) challenge this foundational assumption as they enable individuals to implement their own IT innovations quickly. Placing such empowered individuals into a strictly regulated IT environment will drive them away from the IT department and towards their own IT solutions and inevitably to non-compliance. Such user- or business-driven solutions are not necessarily the result of strict policies or limited user rights but may be caused by the inability of the IT department to fulfil business needs. The phenomenon of user-driven fulfilment of requirements is called Shadow IT (SIT). While receiving very limited scholarly attention, SIT is a widespread challenge amongst IT departments. We employ a triangulation approach using three independent data sources to address this phenomenon within the three domains of IS research, IS Security (ISsec), IT Governance (ITG) and Business IT Alignment (BITA). Our findings suggest that practitioners follow three different ITG approaches to SIT based on their business or IT strategy: IT-control, user-oriented and user-driven.

Keywords: Shadow IT, Non-Compliance, Business IT Alignment, IT Governance, IS Security, Bring Your Own Device, User-driven, Business-Driven

1 Introduction

Napa County is one of the more quiet regions of California and is internationally known for its wine. It is also the home of little more than 130`000 citizens (Wikipedia, 2011), governed by around 1`300 government agents who control a budget of about 315 Million US Dollars (Watt and Schulze, 2011). Although it is a romantic hideout far off the bustling business world, its government has already successfully addressed one of the major information security challenges currently faced by numerous companies. Just like in global corporations (e.g. Credit Suisse (Rusli, 2011) or Barclays Capital (Bansal, 2011)), employees of the Napa Country government had begun infiltrating their business environment with their personal mobile devices insisting on using them instead of the provided infrastructure. Due to a number of local, state and federal regulations, Chief Information Security Officer Gary Coverdale had two choices: Enforce the banning of personal devices or make personal devices compliant to the regulations. After ruling out security concerns, he chose the latter and deployed a device-independent software layer, which allowed employees to securely access the county's IT infrastructure from their private devices (Good Technology, 2011). With this strategy the IT department increased the productivity of the workforce while maintaining data security compliance and reducing costs (Good Technology, 2011).

The case of Napa County is a prime example how the roles of users and IT are changing in today's world of ubiquitous computing (Lyytinen and Yoo, 2001) and the emerging culture of digital natives (Prensky, 2001). Powerful consumer-oriented mobile devices (Lyytinen and Yoo, 2002), broadband mobile internet access and the exploding number of potent web services (Desisto and Pring, 2011), now allow the common users to bypass their company's IT policies and restrictions at their own will (D'Arcy, 2011). At the same time digital natives are quicker to reject user-unfriendly or restricted IS (Prensky, 2001). Hence, the risk that these users will bypass inconvenient IS and find or develop alternate more user-friendly or sophisticated IT solutions to get their work done in their own way, is higher than ever. Another serious example is vividly portrayed by Panko (2006), indicating that usage of decentral spreadsheets has led to an average error rate beyond 90%. The use of spreadsheets instead of centralized solutions can pose a serious data quality risk to companies.
In this paper, we refer to such user-driven IT solutions as ***Shadow IT (SIT) solutions***. SIT solutions (also referred to as "Rogue IT") pose a major financial, legal and reputational threat to organisations as they are not verified to comply with any of the organisation's information security or architectural policies (Behrens and Sedera, 2004). On the contrary SIT allows exploiting user-driven innovation and identifying potential improvements to the existing IS landscape (Behrens, 2009). Based this duality practitioners are discordant how to approach the growing challenge of SIT. Addressing this dilemma this paper presents "consumable research" (Robey and Markus, 1998) by answering the question:

What approaches to SIT are available in literature and are implemented by practitioners?

Since SIT may be addressed in multiple relevant research domains we pose the following additional research questions:

1. ***What ISsec measures are suggested and applied to mitigate the risk of well-intended user-non-compliance (user-driven IT solutions)?***
2. ***What are the key factors that cause Business-IT-misalignment and encourage user-driven IT solutions?***
3. ***What ITG mechanisms are suggested and applied to identify and harness the potential of user-driven IT solutions?***

The paper continues as follows: After conceptualising the phenomenon of SIT in Chapter two, we outline our research methods in Chapter three and present our results in Chapter four. We triangulate our findings in Chapter five and conclude with an outlook to further research in the final Chapter.

2 Conceptualizing Shadow IT

Non-compliance of users with ISsec policies, often referred to as "insider threat" (Warkentin and Willison, 2009), is identified as one of the top ISsec threats in organisations (Computer Security Institute, 2011). "If users do not comply with ISsec policies, ISsec measures lose their efficacy" (Puhakainen and Siponen, 2010, p. 758). Therefore non-compliant user-driven innovations – SIT – pose a security threat in organizations. Based on the taxonomy for ISsec threats developed by Loch et al. (Loch et al., 1992) and expanded by Warkentin (Warkentin, 1995) we classify the threat emerging from SIT as an insider threat which is caused by *internal* (*human*) members of an organization. Furthermore, we chose to address situations where SIT is implemented *intentionally* to support a business process (*low-grade*) and not to maliciously inflict (*high-grade*) economic damage (Warkentin, 1995). Since the phenomenon of SIT is regarded as security threat, we turn to practitioners and researchers of the ISsec domain to ask our first Research Question (RQ1): ***What ISsec measures are suggested and applied to mitigate the risk of well-intended user-non-compliance (user-driven IT solutions)?***

As we approach the classification of SIT above, following question arises: Why would users implement their own IT solutions instead of relying on the solutions provided by the IT department? Behrens (2009) suggests that SIT solutions operate in the fringes of organisations filling a gap between the requirements of the users and the solutions provided by the IT department. This leads us to the domain of BITA.
BITA (considering "alignment" as a state) is a snapshot of an organisations ability to fulfil business needs with IT capabilities (Henderson and Venkatraman, 1993) and to use and harness these capabilities to achieve its business goals (Luftman and Kempaiah, 2007). Poor BITA is caused by either the lack of IT capabilities or the lack of adaptability of business processes or the involved employees. Both cases encourage the development of SIT. When users are unable to adapt to a new ERP system (Jones et al., 2004) or the IT department is unable (or unwilling) to equip all users with custom devices, SIT, in form of user-driven IT solutions (e.g. the usage of an alternate IS or user-owned devices), are likely to appear. This causality leads us to approach the well-established IS research domain of BITA (Chan and Reich, 2007) with our second research question (RQ2): ***What are the key factors that cause misalignment and encourage user-driven IT solutions?***

The ideal state of BITA, where all business needs are fulfilled and all IT potentials are leveraged, however, is hard to accomplish and sustain in practice (Cleven, 2011). In order to fuse IT and business (De Haes and Van Grembergen, 2009) and ensure returns on IT investments (Webb et al., 2006) organisations have deployed ITG instruments containing a mix of structures, processes and relational mechanisms (Weill and Ross, 2004). The goal is to reach the highest level of alignment maturity as described by Luftman (2000), which will foster the ideal state of BITA. As user-driven IT innovations are an indicator for poor alignment and at the same time offer an operational solution, SIT may offer multiple opportunities for ITG practitioners to improve alignment. We therefore explore the domain of ITG with our third Research Question (RQ3): ***What ITG mechanisms are suggested and applied to identify and harness the potential of user-driven IT solutions?***

Armed with a map of relevant IS research fields, namely ISsec, BITA and ITG, and with three research questions to investigate, we now set out to explore these questions in practice and scholarly literature.

3 Research Method

This research article aims at producing consumable research, while committing to practical relevance, and rigorously applying the best suited methodology (Benbasat and Zmud, 1999). To assure relevance scholars are advised to do research *for* practitioners, perhaps even with their financial support (Robey and Markus, 1998). Hence, the results in this paper stem partially from research conducted in the interest of Salesforce.com. Inherent to the origins of the company - growing from a niche web-service

provider to a global player on the IT-market - it is in the interest of salesforce.com to investigate the phenomenon of SIT.
Since there are only few reliable research contributions addressing the phenomenon of SIT directly, we decided to combine available and newly collected data from three different sources. This triangulation of research methods allowed us to illuminate the phenomenon from different perspectives and improve the accuracy of our findings by relying on different kinds of data (Jick, 2011; Denzin, 2009). For a broad understanding of the real-life situation regarding SIT we evaluated multiple practitioner surveys available online. We then continued to identify the current state-of-the-art in scholarly research through a rigorous literature review. Finally, we conducted multiple extracting case studies. Each research methodology is explained in detail in the following paragraphs.

3.1 Practitioner Survey Review

In our attempt to grasp the initial situation we compiled available surveys from established institutions. We believe the selected surveys may not comply with the scholarly rigour but still reflect current challenges. To address the possible bias due to the interests of the sponsoring company, we have outlined the sponsors and their line of business in Table 1. Surveys were identified from references in scholarly literature and internet searches and included in the analysis if they addressed one or more of the research questions proposed in Chapter 2.

Stream	Reference	Region	Sample	Sponsor
SIT	(Smyth and Freeman, 2007)	UK, USA	650	Blue Prism Ltd. (IT Consultancy)
	(Booz Allen Hamilton Inc., 2003)	global	6	Themselves (Strategic Consultancy)
ISsec	(Computer Security Institute, 2011)	USA	351	CSI (Research Institute)
	(van Kessel, 2008)	global	~1400	Ernest & Young (Fin. Consultancy)
	(RSA Security Inc., 2007)	USA	n/a	Themselves (Security Provider)
	(Ponemon, 2009)	USA	967	IronKey Inc. (Security Provider)
DN	(Accenture, 2009)	Germany	570	Themselves (IT Consultancy)
	(IDC, 2011)	global	3000+	Unisys Corp. (Service Provider)
	(Cagemini, 2011)	EU	173	Themselves (IT Consultancy)
	(Escherich, 2011)	global	1000+	Gartner Inc. (IT Advisory)

Table 1. Analysed Practitioner surveys

3.2 Literature Review

To identify the available scholarly literature on SIT we adapted the method of a systematic literature review as outlined by Webster and Watson (2002). Before conducting the literature review we defined its scope based on the taxonomy developed by Cooper (1988) as follows: We focus on research outcomes with the goal to integrate the findings and organize them conceptually. We chose a neutral representation addressing specialized scholars and cover a representative sample of literature. Early exploratory literature searches, using a combination of the keywords “shadow”, “rogue”, “grey”, “information technology” and “information systems” revealed that there are only three scholarly (peer reviewed) publications available in this field, written by Sandy Beherens (2004; 2009). We therefore fell back on the research streams conceptualised in Chapter 2. Our literature review thus focused on the keywords “information security”, “IT alignment” and “IT governance” as the primary set. Since SIT occurs when concepts of these domains fail, we used negating keywords for the second set which thus contained “non-alignment”, “misalignment”, “non-compliance”, “lack of”, “missing” and “poor”. For our search we required one keyword from the first and one from the second set to appear in either title, abstract or keywords of articles. Multiple databases (Ebscohost, Proquest, JSTOR, ScienceDirect and ISI WebOfKnowledge), senior IS journals (based on the AIS senior basket of six containing EJIS, ISJ, ISR, JAIS, JMIS and MISQ) and the proceedings of established international IS conferences

(ECIS, HICSS, ICIS, AMCIS, ACIS and PACIS) have been queried with the described keyword combinations. Additional two iterations of backward searches (Levy and Ellis, 2006) were conducted to identify further literature outside of our initial review scope. The results are presented in detail in Chapter 4.2.

3.3 Extracting multiple case study

To gain insight into the fabric of SIT and how it is perceived and addressed by practitioners we employed the method of case study research which is frequently used to study IS phenomena Palvia et al. (2004). Multiple case studies are described as being robust (Yin, 2003) and allowing better generalisation of the research findings (Benbasat et al., 1987). Van Aken (2004, p. 232) applies the method of the *extracting* multiple case study as a form of "best-practice research, aimed at uncovering technological rules that are already in practice". Since we strongly believe that SIT is a well-known phenomenon amongst practitioners, with little scholarly attention, we conducted an extracting multiple case study with a heterogeneous group of ten Swiss and German organisations. The intentional variety of organisational characteristics (i.e. type, industry, etc.) introduces diversity to our sample. The characteristic of this group are outlined in Table 2.

	A	**B**	C	D	**E**	F	G	**H**	I	J
Type	Public	Public	Private	Public	Private	Private	Private	Private	Private	Private
Industry	Gov.	Uni.	Bank	Bank	Auto.	Engine.	Insurance	Bank	Auto.	Finance
Portfolio	Standard services	Custom projects	Standard service	Standard service	Standard products	Hybrid products	Hybrid services	Standard service	Hybrid products	Standard service
IT Dep.	Central	Decentral	Central	Central	Central	Central	Central	Central	Central	Central
Size	45	3	50	840	750	350	720	2500	60	110
Users	2´500	150	650	5´000	60´000	16´000	7`200	22`000	1`800	4`000

Table 2. Characteristics of our case study partners

Each case study involved one interview with the CIO (with two exceptions: (B) local head of IT, (C) COO) of the organisation and the analysis of internal documents (e.g. portfolios and budgets). Each interview was transcribed and analysed in detail. The semi-structured interviews lasted one hour in average and were based on an interview guideline. The guideline was designed using open-ended questions and was pretested multiple times with practitioners (different from our case study partners). The guideline addressed the following key aspects: (1) practitioners perception of SIT, (2) reasons for SIT, (3) impact of SIT and (4) methods and strategies to identify, institutionalise and avoid SIT. The case analysis was rounded off with a cross-case comparison. The results are described in the following Chapter. Due to multiple requests, all cases are presented anonymously.

4 Research Findings

Our findings are divided according to the results of our three distinct methodological approaches, while the overall essence - the triangulation and synthesis of these results - is presented in Chapter 5.

4.1 Practitioner Survey Findings

Out of the ten studies (see Table 1) two directly address SIT. 67% of the participants, surveyed by Smyth and Freeman (2007), say that SIT is an existing phenomenon in their company and that the main reason is the inability of the IT department to fulfil the business requirements, especially delivery times. The insights described by Booz Allen Hamilton (2003) further mention the lack of clearly enforced policies and the ability to deliver the required quality and/or quantity of services at reasonable cost as possible reasons for SIT.

This risk is also confirmed by the four surveys focusing on IS security, which all stress the eminent and growing risk of non-compliant users. The study conducted by the Ponemon Institute (2009) describes that security policies are increasingly ignored by employees and managers due to the lack of employee training. This is supported by RSA Security (2007), who found that every third employee feels a need to work around security policies to get his job done. Van Kessel (2008), identifies employees as the weakest link for information security and suggests regular security audits. The need for training is highlighted in (Computer Security Institute, 2011), where end-user security awareness training is the only security measure where investments are deemed inadequate.
The increasing number of reports on user non-compliances is fuelled by the emerging culture of the digital natives and their new IT requirements. Accenture (2009) goes as far as to say "golden ages" of SIT are ahead as this new generation will infiltrate corporate. IDC (2011) illustrates that IT departments are misjudging the number of employees using consumer devices for work by nearly 50%. Although IT departments have begun to address the demand for consumer devices (Escherich, 2011) the risk that users or departments simply choose a different service provider online whenever the IT department is not able to fulfil the requirements, is constantly growing (Cagemini, 2011).
From the practitioner survey we derive following insights: (1) Inability to fulfil business needs drives SIT, (2) user non-compliance is the largest ISsec threat, (3) risk from user-non-compliance can be mitigated by user-training, clear and enforced policies and security audits, (4) IT departments are disconnected from their users and (5) IT departments need to adapt their portfolio to suite their users.

4.2 Literature Review Findings

Our literature review has yielded multiple insights into the research streams adjacent to SIT: ISsec, BITA and ITG as outlined in Table 3.

	Database Searches	**AIS Journal Searches**	**Conference Search** (full-text)	**Initial Results**	**Backward Search**	**Total Results**
Hits	216	2	127	345	33	378
Relevant hits	7	2	10	19	33	52
IS Security	6	2	3	11	7	18
Business IT Alignment	1	0	3	4	18	22
IT Governance	0	0	4	4	8	12

Table 3. Results of the literature review

Since security compliance is a major issue on the agenda of *IS security* researchers (Zafar and Clark, 2009), results for the term non-compliance are predominantly found in this research stream (compare Table 3 - "Initial Results"). Recently, multiple methods have been suggested how the risk of the non-compliant employee, referred to as "insider threat" (Warkentin and Willison, 2009), may be mitigated: Employee awareness trainings (Puhakainen and Siponen, 2010), moral reasoning (Myyry et al., 2009) and mandatories and control (Boss et al., 2009). Although the "human factor in information security" (Sauvé et al., 2006) is increasingly being taken into account, the prevalent viewpoint is that it is the employees behaviour that needs to be adjusted and not the IT portfolio or the policies. Out of the sample of analysed articles only Krull (1994) and Ramachandran et al. (2008) stress the necessity to align security measures to changing business, user and cultural needs.
On the contrary, the alignment of the overall IT capabilities with business needs has been widely discussed (Chan and Reich, 2007). Although misalignment is not a popular title our backward search has yielded multiple articles to the causes of misalignment. As SIT emerges at employee level, we focus on factors causing misalignment between lower fields of the alignment model of Henderson and Venkatraman (1993). Reasons for short-term misalignment are the detachment of IT and business employees: Lack of communication (Campbell, 2005; Reich and Benbasat, 2000), decreased responsiveness (Teo and Ang, 1999), invisibility of the IT staff and missing shared knowledge (Earl, 1989). This can either result from a misalignment of the long-term IT strategy with technology forces (Henderson and Venkatraman, 1993), the employee needs (Chen, 2008) and culture (Pyburn, 1983) or

from the time lag between business and IT planning processes while business and IT environment are quickly evolving (Van der Zee and Jong, 1999).
To capture these deficiencies and to enhance alignment, ITG research has emerged. Since the late 90s, concurrent with the wave of IT (re-)centralisation, research in the field of ITG has addressed how to effectively distribute IT decision rights (Weill and Ross, 2004). Multiple interdependent forces need to be taken into account for this decision (Sambamurthy and Zmud, 1999) as it deeply affects the IT capabilities of an organisation. Decentralised IT units have the ability to cater closer to the user needs while a centralised unit has greater potential to achieve economies of scope (Brown and Magill, 1994). Assuming the IT department structure is fixed, ITG research offers multiple practitioner-oriented mechanisms to harmonise business and IT strategies as described by De Haes and Van Grembergen in various publications (2009; 2008), These mechanisms ensure interdisciplinary (business and IT) decisions making, processes which enhance transparency and alignment of the IT department on a strategic level and relational structures to institutionalise the creation of shared knowledge and understanding on the executive level.
In the domains of ISsec, BITA and ITG research we found SIT to be predominantly an ISsec issue in the academic literature. However, ISsec researchers are only addressing it as a form of user non-compliance and hence as a risk that needs to be avoided – answering RQ1. Research in BITA concludes that misalignment occurs through the relational, strategy and structural detachment of IT and business. While all symptoms of misalignment can directly (e.g. invisibility of IT staff) or indirectly (e.g. outdated IT strategy) cause SIT, there is no indication which forms of misalignment are the strongest drivers – answering RQ2. ITG researchers assist in answering the structural question about de- and recentralisation and provide strategic instruments to support BITA. Strategic instruments focus mostly on *how* alignment can be achieved and less on *what* (e.g. policies, portfolio, control mechanisms) needs to be aligned. There are no methods described on how misalignment can be identified (while the maturity of alignment *methods* is measurable by (Luftman and Kempaiah, 2007)) or how its symptoms can be counteracted – failing to answer RQ3. Hence, ITG offers no support to identify and address user-driven IT solution as a result of misalignment. A reoccurring issue in all three research domains is the cultural aspect. Working culture is identified to have a significant impact on business user compliance and their cooperation with IT. Therefore employee culture needs to be taken into account while implementing ITG practices.
While ISSec research has provided one approach to SIT we still lacking approaches which harness the potential of SIT. We therefore take a look at how ten different organisations are handling the phenomenon of SIT in practice.

4.3 Extracting Case Study Findings

Our case studies have revealed three predominant approaches to SIT, which we classify as follows: (1) user-driven, (2) user-oriented, and (3) IT-control. As depicted in Table 4, organisations implement different IT approaches within their service portfolio. The organisations B (approach 1), H (approach 2) and E (approach 3) are highlighted (bold) as they implement the purest forms of the three approaches. We now analyse each approach in detail in the following section.
The **IT-control** approach revolves around the central theme of control and compliance of IT and its usage: *"A CIO can only guarantee IT compliance for a whole organisation if all IT budgets are under his control"* (CIO of E). It is the most commonly mentioned approach to software and hardware services and the dominating mind-set within engineering industries (automotive companies E, I and machine builder J). The goal is to guarantee total transparency and control over all IT solutions implemented within the organisation to fulfil internal and external (e.g. Sarbanes-Oxley Act) compliance and to achieve maximal efficiency at the lowest possible risk. SIT is avoided through technical and employee restrictions (policies) and in the long-run with training and even punishment. Organisations do not hesitate to enforce their policies: "*We had to lay off two people this year for seriously violating IT security polices by installing their own software*" (CIO of A). Since no user-driven innovation is supported, it is a regular challenge for these departments to "*technologically stay ahead of the business units and anticipate their requirements*" (CIO of organisation F). The best way to quickly identify new

requirements is through presence and communication: "*Communication has the highest importance. Our IT coordinators are our eyes and ears in every business unit, so we can respond to new business needs quickly*" (CIO of organisation I). This becomes increasingly difficult where a growing number of business users are supported by stagnating (or decreasing) number of IT staff due to centralisation. This is the case at multiple organisations (A, E and F) with E being the prime example: The ratio of users to IT staff is 80 to 1. At the same time ensuring compliance is regarded a regular challenge within all aspects of their portfolio. We conclude that fully controlling the whole IT portfolio and keeping it aligned with business needs is tremendous effort which is especially difficult to handle in large organisations with a small centralized IT unit. However if mastered successfully the IT risks (e.g. security, under-licencing) can be minimized and the economies of scope for IT (e.g. shared infrastructure and support) can be maximised.

Company	A	**B**	C	D	**E**	F	G	**H**	I	J	Σ ✔	Σ 👁	Σ ✕
Scripting	✔	✔	👁	👁	✕	👁	👁	👁	👁	✔	3	**6**	1
Hardware	👁	✔	✕	✕	✕	✕	✕	✔	✕	✔	3	1	**6**
Software	✕	👁	✕	✕	✕	✕	✕	✕	✕	✕	0	1	**9**
Web Service	**?**	👁	**?**	✕	✕	✕	✕	✕	👁	✕	0	2	**6**
✔ = user-driven, 👁 = user-driven but closely monitored, ✕ = IT controlled, ▒ = poses a regular challenge													

Table 4. Case study results: Support for user-driven IT solutions

The **user-driven** approach shifts the responsibility for IT innovations from the IT department to the business user: *"Although shadow IT is often perceived as problem, it is the main innovation driver within our organisation"* (local head of IT of university department B). Although it is rare that this approach is applied to the overall portfolio (only witnessed at organisation B), it is the common approach to scripting (incl. macros) in most organisations. The goal is to boost the effectiveness of IT usage by supporting whatever solution users see best fit and embracing the security risk emerging from user empowerment. SIT is therefore regarded as a form of innovation enhancing the effectiveness of employees. The challenge with SIT is seen in keeping up with it rather than avoiding it. To achieve this, organisations "*have a dedicated budget to integrate user-driven solutions (scripts), which become business-critical*" (CIO of H). On a hardware, software and web service level SIT poses a "*large security risk*" (local head of IT at B) as avoiding data-leakage becomes the "*personal responsibility of the users*" (CIO at J). Hence, at B the local IT department relies on empowered users to secure their own working environment and focuses on protecting the centralised infrastructure and services according to web standards. However, such *"empowerment requires high user IT skills and an aware and responsible mind-set and high security set-up costs for infrastructure and services"* (local head of IT at B). We conclude that the user-driven approach enhances innovation and efficacy of IT usage, while increasing IT security risks and integration costs and limiting economies of scope to a small set of provided services. Costs may be reduced through the empowerment of employees, but requires a certain employee mind-set and skill. As we only witnessed the user-driven approach for the overall portfolio at university B, we acknowledge that this may only be feasible for small organisations.

The **user-oriented** approach combines the advantages of the IT-control and the user-driven approach by applying them differently throughout their portfolio: *"While transparency is my highest priority, I do believe that a healthy extent of SIT is essential to offer flexibility and space for new ideas and innovation"* (CIO of organisation H). This approach is common to organisations supporting Bring Your Own Device (BYOD) campaigns, while maintaining a controlled environment (H, J). The goal is to maintain efficiency and supporting user-driven innovation at reasonable risk. SIT is therefore encouraged within and avoided outside defined boundaries (see Table 4, H and J supporting user-driven devices, while strictly controlling software and web services). Multiple companies (A, C, F, H, J) acknowledge to accommodate "*isle or small solutions, which are developed or sourced by the business and supported by the IT department but hardly fit in with the overall architecture*" (CIO at F) or are "*adopted to quickly and temporarily serve a certain functionality within a business department*" (CIO at C). To allow these solutions exceptions to policies (waivers) are defined. *"If our designers want*

Macs, then they shall have them. But they need to be responsible for security, operation and support themselves, as we only provide them with the basic infrastructure" (CIO at J). Similar to BYOD campaigns IT departments in these situations offer security, support and continuity up to a defined and standardised interface beyond which uncontrolled user-driven solutions, hence SIT is allowed to develop. This requires services to support sophisticated security measures (to allow safe access via internet) and a standardised interface (to support multiple devices). This involves high set-up costs (mentioned at B, C, H, J and I) which not all companies can afford. We conclude that the user-oriented approach can be adapted to balance efficient operation and the effective use of IT through user-driven innovation within defined boundaries. However the level of freedom differs within the interviewed organizations. To apply this approach a thorough risk assessment (Benaroch et al., 2006) is suggested beforehand to define the boundaries of user innovation. For this we suggest to apply the follow list of risks associated with SIT.

Independent of their approach to SIT we queried the organizations to identify the major risks resulting from SIT. The most common cited risks were: *Data security and compliance, efficiency and synergy losses, lacking continuity and the disruption of a controlled enviroment*. While data security has been already extensively discussed earlier in this paper, efficiency losses through redundant solutions and reduced data quality is evaluated by Panko (2006). Disrupting the controlled IT enviroment introduces an unpredictible risk. This also leads to the inability of the IT department to guarantee long-term support (continuity) for such an unpredictable enviroment.

Although we were hoping to find a link between our case study subjects' approach to control (as described above) and their lacking capabilities which lead to SIT, no correlation was found. The most common deficiencies of the IT departments driving SIT were identified to be: *IT adaptability to business processes, competitive time to market, business prototyping abilities and low initial cost***.** These findings do, however, portray the most common forms of misalignment, which may drive SIT in organisations. The adaptability of IS to user needs and business processes outlines the well-known tension between the goals of maximising efficient operation and supporting effective use of IT. The other three capabilities highlight the pressure on IT departments emerging from the growing number of web based service providers. This enables users to try multiple solutions (prototyping) before committing to one. Our case study partners suggest that as business becomes growingly aware of these possibilities, time and cost for implementing solutions within IT departments, become critical drivers for SIT.

From our case study research we conclude that the way organisations approach the phenomenon of SIT reflects their strategic goals. IT-control: maximal efficiency and minimal risk; user-driven: maximal effectiveness and innovation accepting an intransparent risk; user-oriented: efficiency and transparent risk is in balance with effectiveness and innovation. SIT can therefore be regarded as both a threat and an opportunity. Further, we have derived the top four business needs that drive SIT when not addressed: Adaptability of IS to business users and processes, implementation time of IS, initial cost of new IS and the inability to evaluate the impact of new IS through prototyping. How these findings relate to insights gained form the practitioner and the knowledge base in scholarly literature is discussed in the following Chapter.

5 Triangulation of Findings

We now combine our findings, derived from our three independent sources described in Chapter 4, to gain more detailed insights to the phenomenon SIT. Practitioner surveys set the scene by describing the challenge of SIT, alignment and user non-compliance in the new age of digital natives and ubiquitous computing. However the surveys fail to capture a holistic approach to SIT. Scholarly literature on ISsec offers holistic approaches to security by providing strategies to identify and implement the most effective means of user control. Although not considered within ISsec literature, failure to fulfil critical business needs drives SIT, as suggested by the practitioner surveys and confirmed by our case study findings. BITA literature offers concepts to improve on such misalignments holistically. ITG literature extends institutionalizes these concepts. While SIT offers multiple ways to improve BITA hence ITG mechanisms it has so far been disregarded in both domains of research. Our case studies

findings close this gap by providing three ITG approaches to SIT: IT-control, user-oriented and user-driven. Each supports a unique combination of strategic goals in terms of efficiency, risk, effectiveness and user-driven innovation.

6 Conclusion, Limitations & Outlook

We have leveraged three different sources to understand and conceptualise the phenomenon of SIT and discovered that practitioner approach to SIT is depending on their strategic orientation. Approaches can be divided into three groups: *IT-control*, *user-orientated* and *user-driven*. While the first approach rules out SIT as a risk-factor, the other two approaches leverage the potential of user-driven IT innovations inherent to SIT. Hence, we question the phenomenon of SIT to be merely a security control and risk issue.

Within these approaches, practitioners combine elements of ISsec, ITG and BITA, while researchers address these domains as distinct research silos. To address new practitioner challenges, such as SIT, we suggest that researchers must remix insights from multiple IS domains. Although we believe to have covered the most relevant IS domains for SIT we deliberately chose not address the neighbouring research streams of Risk Management, Enterprise Architecture, Portfolio Management or Continuous Improvement. Further research may thus reach out to these IS domains and extend our ITG approaches. To conclude this paper, we return to the wine fields of Napa County. With the insights of our research the shift in the IT strategy of Napa Counties government can be explained. Coming from an *IT-control* approach, the IT department was confronted with a growing demand for individual user devices which could not be fulfil by the IT department alone. A *user-oriented* approach was adapted by allowing mobile devices to be chosen (and financed) by the employees themselves. These devices are part of an uncontrolled user-driven IT environment, or Shadow IT, which enhances the employee's freedom and boosts their effectiveness.

References

Accenture (2009). "Millennials vor den Toren" – Anspruch der Internet-Generation an IT. 13.

Bansal, P. (2011). BlackBerry outage frustrates investment bankers. Reuters, 1.

Behrens, S. (2009). Shadow Systems: The Good, The Bad and the Ugly. Communications of the ACM, 52, 124-129.

Behrens, S. and Sedera, W. (2004). Why Do Shadow Systems Exist after an ERP Implementation? Lessons from a Case Study. In Pacific Asia Conference on Information Systems, 1713-1726.

Benaroch, M., Lichtenstein, Y. and Robinson, K. (2006). Real Options in Information Technology Risk Management: An Empirical Validation of Risk-Option Relationships. MIS Quarterly, 30

Benbasat, I., Goldstein, D. K. and Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. MIS Quarterly, 11, 369-386.

Benbasat, I. and Zmud, R. W. (1999). Empirical Research in Information Systems: The Practice of Relevance. MIS Quarterly, 23, 3-16.

Booz Allen Hamilton Inc. (2003). Shining the Light on Shadow Staff. Understanding and Minimizing Hidden Staff Costs. 1-8.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A. and Boss, R. W. (2009). If someone is watching , I'll do what I'm asked : mandatoriness, control, and information security. European Journal of Information Systems, 18, 151-164.

Brown, C. V. and Magill, S. L. (1994). Alignment of the IS Functions with the Enterprise: Toward a Model of Antecedents. MIS Quarterly, 18, 371.

Cagemini (2011). Studie IT-Trends 2011 Unternehmen fordern wieder Innovation. Capgemini, 1-40.

Campbell, B. (2005). Alignment: Resolving ambiguity within bounded choices. In Pacific Asia Conference on Information Systems, 1-14.

Chan, Y. E. and Reich, B. H. (2007). IT alignment: what have we learned? Journal of Information Technology, 22, 297-315.

Chen, H.-M. (2008). Towards Service Engineering: Service Orientation and Business-IT Alignment. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), 114-114, Ieee.
Cleven, A. (2011). Exploring Patterns of Business-IT Alignment for the Purpose of Process Performance Measurement. In European Conference On Information Systems, 1-12.
Computer Security Institute (2011). CSI Computer Crime and Security Survey 2010/2011. Computer Security Institute, New York, 1-42.
Cooper, H. M. (1988). Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews. Knowledge in Society, 1, 104-126.
D'Arcy, P. (2011). CIO strategies for consumerization: The future of enterprise mobile computing. Dell CIO Insight Series. Dell Inc., 1-15.
De Haes, S. and Van Grembergen, W. (2008). Analysing the Relationship Between IT Governance and Business/IT Alignment Maturity. In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, 428-428, IEEE.
De Haes, S. and Van Grembergen, W. (2009). An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment. Information Systems Management, 26, 123-137.
Denzin, N. K. (2009). The research act: a theoretical introduction to sociological methods. Aldine Transaction, New Brunswick, NJ.
Desisto, R. P. and Pring, B. (2011). Essential SaaS Overview and 2011 Guide to SaaS Research. Gartner, 1-16.
Earl, M. J. (1989). Management strategies for information technology. Prentice Hall.
Escherich, M. (2011). Search Analytics Trends: The Inevitable Consumerization of Corporate IT. Gartner, 1-5.
Good Technology (2011). Case Study of Napa Country. Good Technology, 1-3.
Henderson, J. C. and Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. IBM Systems Journal, 32, 4-16.
IDC (2011). Unisys Consumerization of IT Benchmark Study. UNiSYS, 1-38.
Jick, T. D. (2011). Mixing Qualitative and Quantitative Methods : Triangulation in Action. Administrative Science Quaterly, 24, 602-611.
Jones, D., Behrens, S., Jamieson, K. and Tansley, E. (2004). The Rise and Fall of a Shadow System: Lessons for Enterprise System Implementation. In ACIS'04, 1-12.
Krull, A. R. (1994). Strategic Misalignment - How organizations can survive information security. Computer Fraud & Security Bulletin, 11-19.
Levy, Y. and Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. Informing Science Journal, 9, 181-212.
Loch, K. D., Carr, H. H. and Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. Management Information Systems, 16, 173-186.
Luftman, J. (2000). Assessing Business Alignment Maturity. Communications of the Association for Information Systems, 4, 1-51.
Luftman, J. and Kempaiah, R. (2007). An Update on Business-IT Alignment: "A Line" Has Been Drawn. MIS Quarterly Executive, 6, 165-177.
Lyytinen, K. and Yoo, Y. (2001). The Next Wave of Nomadic Computing: A Research Agenda for Information Systems Research. 377-388.
Lyytinen, K. and Yoo, Y. (2002). Issues and Challenges in Ubiquitous Computing. Communications of the ACM, 45, 63-65.
Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems, 18, 126-139.
Palvia, P., Mao, E. and Midha, V. (2004). Research Methodologies in MIS: An Update. Communications of the Association for Information Systems, 14, 526-542.
Panko, R. R. (2006). Spreadsheets and Sarbanes-Oxley: Regulations, Risks, and Control Frameworks. Communications of the Association for Information Systems, 17, 1-50.

Ponemon, L. (2009). Trends in Insider Compliance with Data Security Policies. Ponemon Institute.
Prensky, M. (2001). Digital Natives, Digital Immigrants. On the Horizon, 9, 1-6.
Puhakainen, P. and Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly, 34, 757-778.
Pyburn, P. J. (1983). Linking the MIS plan with corporate strategy: an exploratory study. MIS Quarterly, 7, 1-14.
Ramachandran, S., Rao, S. V. and Goles, T. (2008). Information Security Cultures of Four Professions: A Comparative Study. In HICSS 08, 1-10.
Reich, B. H. and Benbasat, I. (2000). Factors That Influence the Social Dimension of Alignment between Business and Information Technology Objectives. MIS Quarterly, 24, 81-113.
Robey, D. and Markus, M. L. (1998). Beyond rigor and relevance: producing consumable research about information systems. Information Resources Management Journal. Idea Group Inc.
RSA Security Inc. (2007). The Confessions Survey: Office Workers Reveal Everyday Behavior That Places Sensitive Information at Risk. RSA Security Inc., Bedford, MA (USA), 1-12.
Rusli, E. M. (2011). Wall Street's 'CrackBerry' Withdrawal. The New York Times, 1.
Sambamurthy, V. and Zmud, R. W. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies. MIS Quarterly, 23, 261-290.
Sauvé, J., Moura, A., Sampaio, M., João, J. and Radziuk, E. (2006). An Introductory Overview and Survey of Business-Driven IT Management. In Business-Driven IT Management, 1-10, IEEE.
Smyth, K. and Freeman, J. (2007). Blue Prism Rogue IT Survey 2007. Blue Prism, 1-5.
Teo, T. S. H. and Ang, J. S. K. (1999). Critical success factors in the alignment of IS plans with business plans. International Journal of Information Management, 19, 173-185.
van Aken, J. E. (2004). Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules. Journal of Management Studies, 41, 219-246.
Van der Zee, J. T. M. and Jong, B. d. (1999). Alignment is not enough: Integrating business and information technology management with the balanced business scorecard. Journal of Management Information Systems, 16, 137-156.
van Kessel, P. (2008). Moving beyond compliance. Ernst & Young's 2008 Global Information Security Survey. Ernst & Young, 1-34.
Warkentin, M. and Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems, 18, 101-105.
Warkentin, M. E. (1995). Informations Systems Security and Privacy. In: Advances in Telematics. Volume 3 (Hanson, J. and Liebowitz, J., Eds), 57-79, Ablex Pub. Corp., Norwood, N.J.
Watt, N. and Schulze, T. A. (2011). County of Napa, State of California. Adopted Budget, Fiscal Year 2011/2012. County Executive Office, 1-862.
Webb, P., Pollard, C. and Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly? In Proceedings of the 39th Annual Hawaii International Conference on, 194a-194a, IEEE.
Webster, J. and Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, 26, xiii-xxiii.
Weill, P. and Ross, J. W. (2004). IT Governance. How Top Performers Manage IT Decision Rights for Superior Results. First edit. Harvard Business Press.
Wikipedia (2011). Napa County, California. Wikipedia, 1-15.
Yin, R. K. (2003). Case Study Research. Design and Methods. Third Edit. Sage Publications, Thousand Oaks, London, New Delhi.
Zafar, H. and Clark, J. G. (2009). Current State of Information Security Research In IS. Communications of the AIS, 24, 557-596.