CLOUD STRIFE

MARC HULSEBOSCH
M.A.C.HULSEBOSCH@ALUMNUS.UTWENTE.NL

An analysis of Cloud-based Shadow IT and a framework for managing its risks and opportunities

Master of Science- Business Information Technology
Faculty of Electrical Engineering, Mathematics and Computer Science
University of Twente

February 25, 2016 – version 0.6

SUPERVISORS:
Dr. Klaas Sikkel- University of Twente
Dr. ir. Hans Moonen- University of Twente
Edwin Sturrus, MSc.- KPMG

LOCATION:
Enschede

SUMMARY

This thesis proposes a framework for the management of unauthorized cloud computing usage, based on a risk analysis, a set of possible strategies and concrete measures.

The rise of cloud computing in the consumer domain has raised users' expectations about the types of services that organizational IT departments deliver and the speed of delivery. Many IT departments are unable to keep up with these expectations. As a result, individual employees and departments choose to bring cloud services into the organization by themselves, circumventing IT. This is called Cloud-Based Shadow IT.

The use of these services may result in various risks for the organization, such as business continuity risks, unauthorized access to sensitive data, non-compliance and adverse effects on financial and operational performance. On the other hand, an employee's legitimate desire to use these tools to improve the quality of their works can lead to various benefits.

No frameworks for the management of the risks and benefits of Cloud-Based Shadow IT previously existed, so this report proposes one.

The proposed framework consists of three steps that organizations should follow.

First: analyze how they are impacted by the aforementioned risks, and how they benefit from the positive effects. They should also consider what causes their employees to adopt Cloud-Based Shadow IT.

Second: choose a strategy. Coming from a state of ignoring unauthorized cloud usage, they can choose to monitor which applications are used, accepting both risks and benefits. Going further, they could use blacklisting or whitelisting to select which applications can and cannot be used, balancing risks and benefits.A final option is to prohibit the use of Cloud-Based Shadow IT completely.

Third, they should choose what measures they take, and how they implement them, in accordance with that strategy. This report introduces measures in five steps: prevention, detection, analysis, response and evaluation, and analyzes how Cloud Access Security Brokers (CASBs) and Identity&Access-Management-as-a-Service (IAMaaS)-solutions can be used in these efforts.

The framework has successfully been validated with experts. Since the framework takes a high level perspective of Cloud-Based Shadow IT, the main recommendations are that further research provides additional details about implementation and effectiveness of the proposed measures, that the framework is expanded to better cover various organization sizes, industries, geographies, maturity levels and IT governance models.

ACKNOWLEDGMENTS

This thesis marks the end of my 7.5 years as a student. Fittingly, it also took 7,5 months to write. Even though 7.5 months that is slightly longer than what is is supposed to be, I do believe that it was a smooth ride.

This is primarily thanks to the three people who have guided me: Klaas Sikkel and Hans Moonen on behalf of the University of Twente, and Edwin Sturrus on behalf of KPMG.

I am glad that Klaas and Hans agreed to be my supervisors, even before I knew exactly what I was going to do. I have heard from many other graduates the importance of having supervisors that you can work well with, and who are willing to regularly go through your work both on a high level and with a fine comb. Thank you for that, and for all the previous moments we worked together!

I also grateful that Edwin agreed to be my supervisor at KPMG, where he took the time to discuss my progress at least once a week. Edwin, thank you for both leaving a lot of room for me to figure out where to go, to fail and recover, and for providing professional input in an academic field where business sets the pace.

I also thank Olga Kulikova for reading along several times, for providing a fresh view on the project and for involving me in the discussion on and with CASBs, which was very useful in writing this thesis.

I wrote this thesis as a Graduate Intern at KPMG's Information Protection Services team. I am grateful to them for the opportunity to do so and for letting me be a part of the team by being part of a project and all of the social activities. I could not have wished for more a team of colleagues that was more passionate about what they do, more professional and capable in how they do it and more fun to work with while they do it.

Ruud Verbij, also part of that team, deserves special mention here for pointing me towards this subject and for quickly arranging meetings with Edwin and others to get me started.

I would like to thank my friends, girlfriend, roommates and family (list is not MECE) for supporting me, for sometimes asking how things were going, and for sometimes not asking how things were going.

Finally, I would like to thank the folks at Overleaf for providing me with the Cloud-based Shadow IT used to write this thesis, André Miede for saving me the work of lay-outing it, and Square Enix for the inspiration for the title and the logo.

Marc Hulsebosch
Amstelveen, February 2016

CONTENTS

1 INTRODUCTION 1

2 BACKGROUND 3
2.1 Problem statement 3

3 RESEARCH DESIGN 5
3.1 Research objective 5
3.2 Research questions 5
3.3 Literature review 6

4 DEFINITIONS 9
4.1 Definition of Cloud Computing 9
4.2 Definition of Shadow IT 12
4.3 Definition of Cloud-Based Shadow IT 13

5 CAUSES AND EFFECTS OF CLOUD-BASED SHADOW IT 15
5.1 Causes 15
5.2 Effects 19
5.3 Chapter Summary 27

6 METHODS FOR MANAGING CLOUD-BASED SHADOW IT 29
6.1 Prevention 30
6.2 Detection 33
6.3 Analysis 34
6.4 Response 36
6.5 Evaluation 37
6.6 Commercial products 38
6.7 Chapter Summary 41

7 STRATEGIES REGARDING CLOUD-BASED SHADOW IT 43
7.1 Ignoring 43
7.2 Monitoring 44
7.3 Blacklisting 46
7.4 Whitelisting 49
7.5 Prohibiting 51
7.6 Chapter Summary 51

8 VALIDATION 53
8.1 Interview 1 - CASB Provider 53
8.2 Interview 2 - Professional services firm 54
8.3 Interview 3 - Municipality 55
8.4 Interview 4 - Construction conglomerate 56
8.5 Summary and discussion 58

9 CONCLUSION 61
9.1 Causes and Effects 61
9.2 Measures 62
9.3 Strategies 63
9.4 Answering the main research question 63
9.5 Validation 64

10 DISCUSSION 65
10.1 Contributions to science 65
10.2 Contributions to practice 65
10.3 Limitations and future work 66
10.4 Personal reflection on the project 67

BIBLIOGRAPHY 69

LIST OF FIGURES

Figure 3.1 Phases, inputs and outputs of this research 7
Figure 4.1 Traditional IT and the three cloud computing service models as defined by [46] 11
Figure 5.1 An overview of the categories of causes and effects found as an answer to Knowledge Question 1 15
Figure 6.1 The measures discussed in this chapter 30
Figure 6.2 Shadow IT portfolio plot by Zimmermann et al. [72] 36
Figure 7.1 The five strategies explained in this chapter 43
Figure 7.2 Overview of the framework 44
Figure 9.1 An overview of the categories of causes and effects found as an answer to Knowledge Question 1 62
Figure 9.2 The measures discussed in chapter 6 62
Figure 9.3 The five strategies explained in chapter 7 63
Figure 9.4 Overview of the framework 64

LIST OF TABLES

Table 3.1 Overview of articles found in the various phases of literature research 7
Table 5.1 Overview of causes of Shadow IT as identified in literature and interviews 19
Table 5.2 Overview of negative and positive effects of Shadow IT (SIT) as identified in literature and interviews 26
Table 6.1 Mapping of process steps to other frameworks 29
Table 6.2 Different scenario's where control is required and the applicable CASB integration methods. 40
Table 6.3 An overview of how both causes and effects of Cloud-Based Shadow IT (CBSIT) are impacted by the measures proposed in this chapter 42

ACRONYMS

SIT Shadow IT

CBSIT Cloud-Based Shadow IT

BITA Business-IT Alignment

BYOD Bring-your-own-Device

BYOA Bring-your-own-App

SOX the Sarbanes-Oxley act

VPN Virtual Private Network

PII Personally Identifiable Information

PCI Payment Card Information

PHI Protected Health Information

DLP Data Leakage Prevention

API Application Programming Interface

DNS Domain Name System

IP Internet Protocol

CASB Cloud Access Security Broker

CDP Cloud Data Protection

CSP Cloud Service Provider

IAMAAS Identity&Access-Management-as-a-Service

SAML Security Assertion Markup Language

CISO Chief Information Security Officer

1 INTRODUCTION

IT departments of large enterprises have long been on the forefront of innovation, providing the organization's employees with technology that consumers sparsely had access to.

Those roles have reversed: the cutting edge of technological advances is now in the area of consumer technology, and users expect similar easy to use, turnkey solutions to be available whenever they encounter a task their current tool set doesn't support.

Cloud computing (see section 4 for definitions) is also one of those technologies used by consumers that employees expect to see in their workplace, and that they are quick to introduce if their employer doesn't [39].

Meanwhile, the trend to buy services outside core competences, instead of providing them in-house, had already led many organizations from in-house maintenance of IT services, via outsourcing to increasingly using cloud computing: buying these services from Cloud Service Providers (CSPs). Still, users seem to demand functionality from the cloud that organizations do not yet offer, and thus provide it themselves.

This usage of cloud computing creates a phenomenon called Cloud-Based Shadow IT (CBSIT), where cloud technology is being fielded without the IT department knowing. Although Shadow IT (SIT) has been a concern for two decades [55], CBSIT introduces both specific challenges and opportunities. This thesis looks at the concept of CBSIT, and how organizations should act on it.

2

BACKGROUND

This section presents high-level background information in order to familiarize the reader with the subject matter and provide a line of reasoning towards the choice of the problem that is made explicit in the final section of this chapter. The method used to gather the materials used in writing this chapter is described in section 3.3.

As the introduction states, the rise of CBSIT confronts organizations with new challenges based on the nature of cloud computing.

One of these challenges is the ubiquity: Skyhigh Networks, a provider of tools to manage cloud based SIT, found that many customers underestimate the number of cloud services in use by a factor of 10, with some firms using over 1.000 services according to scans [56]. One survey states that one in five users surveyed used Dropbox, a cloud storage service, at work [17].

Contrary to many traditional SIT systems, cloud solutions do not require much setting up. Many of them are free, and paid services are often quickly procured using just a credit card. They do not require specific hard- or software and often run on various (mobile) operating systems, using the internet.

A short literature scan reveals that CBSIT carries some of the same risks that traditional SIT brought with it, but also poses new risks as it is based on cloud technology. These new risks require that organizations take new measures to control them.

In many areas, widely accepted frameworks exist to provide organizations with a structured approach to be in control of the risks that they face. Such a framework would function to show the organization's desired state (i.e. what degree of usage and associated risk do we deem desirable/acceptable?) and that it has taken appropriate measures to match actual usage to that desired state if required.

2.1 PROBLEM STATEMENT

According to an initial literature search, reading of general publications and discussions with experts, no existing framework as described in the previous paragraphs currently covers CBSIT.

Many frameworks cover one of two topics:

- Traditional shadow IT, covering rogue hardware and software installed on devices without permission from the organization's IT department

- Cloud computing, meaning they cover controls for procurement, roll out and management of cloud solutions through the organization's IT department.

Many of those frameworks contain components that seem useful at a first glance, such as the Critical Security Controls from Center for Internet Security [10]. However, no framework explicitly and completely addresses the issue of CBSIT. The problem considered in this research is therefore a design problem: how to design a framework for the management of CBSIT?

3 RESEARCH DESIGN

This section describes the objective of this research, as well as its division in a design and a knowledge problem. This distinction comes from design science, a research paradigm [68].

3.1 RESEARCH OBJECTIVE

The objective of this research is to help organizations to manage CBSIT by designing a framework that outlines necessary steps to demonstrate control over usage of cloud computing in their organization.

This requires answering a series of knowledge questions. The first aims to get a better overview of the phenomenon CBSIT, while the last three aim to gather more information for the components of the framework.

3.2 RESEARCH QUESTIONS

The main research question below paraphrases the design objective of this research into a research question. Validation of the designed artifact should result in the artifact being the answer to this question.

> RQ: What is a framework that helps organizations control Cloud-Based Shadow IT?

In order to complete the design objective that is embedded in the main research question, it is necessary to answer three knowledge questions, stated below.

1. What are causes and effects associated with Cloud-Based Shadow IT?
2. What are measures for managing Cloud-Based Shadow IT?
3. What are strategies for managing Cloud-Based Shadow IT and how can they incorporate the measures from Question 2?

These questions are answered by performing both literature research and expert interviews.

The experts interviewed are the following:

- The former Chief Information Security Officer (CISO) for an intergovernmental organization [22]
- The former CISO for a large Dutch bank [21]
- The Information Security Officer of a professional services firm [31]
- A product specialist at the Ministry of Defense [51]

The semi-structured interviews were conducted using a short interview protocol, intended to ask open ended questions in order to allow the interview to focus on areas where interviewees wanted to go in-depth.

The interviews were recorded as digital audio files if the interviewees gave consent to do so. The audio files were then partially transcribed where relevant. In the case that the interviewee did not give consent as they felt the interview might cover confidential information, transcription took place during the interview and the interviewee was given the option to review the transcript to ensure it was in accordance with their opinion and did not disclose confidential information.

While answering the last research question in chapter 7, the answers are integrated to form the framework that answers the main research question.

After the framework is created, an additional round of interviews is conducted with experts in order to validate the findings and the framework that was designed. These experts were explained the answers to the knowledge questions and the framework that followed from that.

The experts interviewed are:

- A Director of Sales Engineering at a CASB vendor[18]
- The Information Security Officer of a professional services firm [32]
- The CISO of a Dutch municipality [13]
- The interim Information Security Officer of a construction materials conglomerate [30]

During the first two interviews, general feedback on the framework is gathered, both from the perspective of a vendor whose products aim to be a part of resolving the challenges surrounding CBSIT and from the perspective of a security professional in an organization that advises clients on this topic.

The last two cases can be used to test whether the framework fits within organizations, by asking them to compare their current and desired efforts with the framework.

Any lessons learned from validation interviews and the cases are then used to improve the framework.

The whole process is summarized in figure 3.1.

3.3 LITERATURE REVIEW

In order to assess the current state of the field, I performed a literature review. Based on the method for gathering relevant literature described by Wolfswinkel et al. [69], this literature review started with a selection of databases. In this case, the databases were Scopus and Google Scholar; based on Scopus' larger database and greater coverage of Computer Science and Information Systems compared to its peers (e.g. Web of Science) and Google Scholar's easy to use interface and ability to search "gray" sources (e.g. books, theses and white papers).

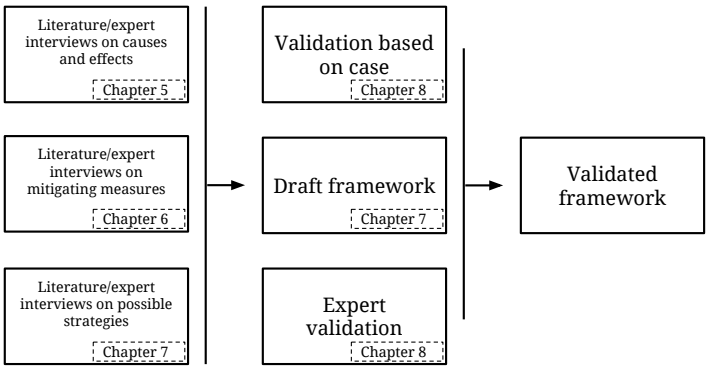

Figure 3.1: Phases, inputs and outputs of this research

Phase	Articles used in research
Initial search	90
Forward and backward searches	54
Other	44
Total	188

Table 3.1: Overview of articles found in the various phases of literature research

In addition to these scientific databases, queries were also performed on the general Google search engine, in order to obtain state of the art work that has not been described in scientific literature yet.

The materials found were then filtered based on their title, keywords and abstract, and later filtered based on whether the full text proved to be relevant. Finally, after compiling a list of relevant articles, each item was subjected to a backward and forward citation search, meaning that the sources that the article cited were examined, as well as any later publications citing the article in question. Although the process described above seems linear, it is in fact an iterative process, where an article found through forward and backward citation check may yield materials that introduce new synonyms or concepts warranting a new database search. By filtering the results of these new searches to stay focused on the topic, new searches resulted in fewer and fewer new articles, until the review could be considered complete. Table 3.1 gives an overview of how many articles were used (i.e. full text retrieved and read) in each phase of the research. Note that not all used articles were cited and thus included in the bibliography in appendix 5.

4 DEFINITIONS

In order to understand the research subject at hand and in order to choose an adequate scope, definition were extracted from literature and used in the previous section. The following section provides definitions for the key concepts under consideration.

4.1 DEFINITION OF CLOUD COMPUTING

The definition of cloud computing most often used is the one provided by the American National Institute for Standards and Technology (NIST):

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
> NIST [46]

NIST proceeds to list five essential characteristics of cloud computing, as well as models of deployment and service models. These are described below, starting with the essential characteristics of a cloud computing service:

On-demand self-service

> A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

> Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

> The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but

may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

The characteristics above describe some of the properties that are essential for a service to be considered a cloud computing service. The precise way in which these properties are implemented varies. NIST therefore provides some service and deployment models which can be used to group cloud services.

First, there are three service models. A graphical representation can be found in 4.1, and they are explained below:

Infrastructure as a Service

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user- specific application configuration settings.

Platform as a Service

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

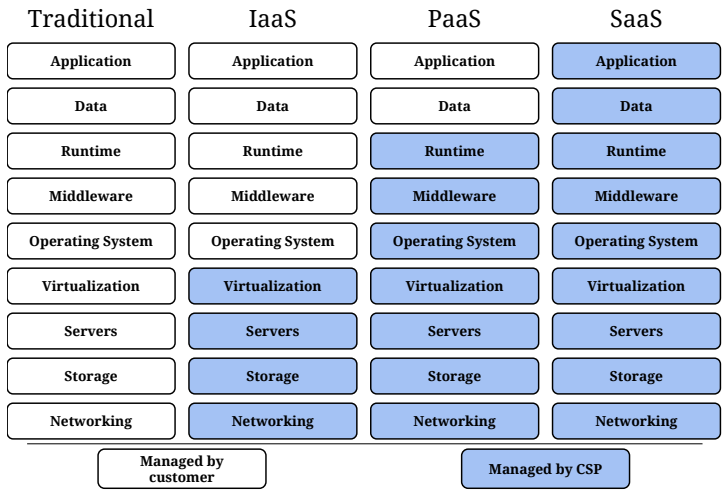

Figure 4.1: Traditional IT and the three cloud computing service models as defined by [46]

Software as a Service

> The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

In practice, the distinction is less precise. For example, some CSPs provide the stack up including an operating system, but none of the parts above.

Public cloud

> The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them.It exists on the premises of the cloud provider.

Community cloud

> The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Private cloud

> The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

In addition, companies can employ multiple cloud services linked together to form a hybrid cloud:

HYBRID CLOUD

> The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

4.2 DEFINITION OF SHADOW IT

With different authors writing on the subject over the years, several definitions of shadow IT exist. One definition is used repeatedly and covers the essence of the subject well:

> Shadow IT represents all hardware, software, or any other solutions used by employees inside of the organizational ecosystem which have not received any formal IT department approval.
>
> Behrens [2], Gyoery et al. [25]

One caveat with the use of this definition is that it speaks of "IT department approval", while the use of IT in many organizations is also governed by a CISO, who is often in a risk management department. This is especially relevant when looking at managing the risks of CBSIT.

Shadow IT can exist in various forms. Shadow IT in the form of spreadsheets (e.g. Excel), sometimes with macros, has been around since these productivity tools became common in the workplace. Going even further, business units have developed applications and client-server systems to solve their problems[18]. Shadow systems may also consist of off-the-shelf products. Cloud-services fall into this category as well.

Another distinction that can be made is whether or not the shadow services are used by employees or departments with the intention to sell them as products, use them to sell products, or sell a product that is largely based on them. Examples would be a team at a retailer developing a shopping app for mobile devices, or an advisory organization where teams create hardware of software solutions that form the basis for services provided to their clients. Looking at the work of Berray and Sampath [5], these solutions would fall under a CTO of the fourth category, whereas the stricter interpretation would place under a CIO. I have decided to place examples of the former out of scope when including them would significantly alter findings.

4.3 DEFINITION OF CLOUD-BASED SHADOW IT

By taking the definition of shadow IT with aforementioned modifications and referring to the definition of cloud computing, the following definition of Cloud-Based Shadow IT emerges:

> Cloud-Based Shadow IT represents all cloud computing-based services used by employees inside of the organizational ecosystem which have not received any formal organizational approval.

As an opposite of this, this report will call applications that have received such approval "sanctioned services", "approved services" or "official services".

5 CAUSES AND EFFECTS OF CLOUD-BASED SHADOW IT

The first knowledge question defined in the research design was

> KQ1: What are causes and effects associated with Cloud-Based Shadow IT?

To answer this question, both literature and experts have been consulted. The sections provide an integrated overview of the outcome of these steps, and the final section provides a summary of key findings. As described in the problem statement, the rise of CBSIT introduces new risks on top of those already posed by traditional SIT. This section will first explore risks traditionally associated with SIT, discussing whether or not they apply to the same extent for CBSIT. It will then continue with an exploration of new risks, specific to CBSIT. An overview of the findings is presented in figure 5.1.

As it turns out, many authors are rather brief or abstract about the causes or effects they state to be associated with shadow IT. In these cases, sources outside the literature found using the method outlined in section 3.3 were searched in order to clarify these phenomena.

5.1 CAUSES

A reading of literature resulted in over thirty phrases that various authors use to identify causes of shadow IT. These are grouped into eight remaining

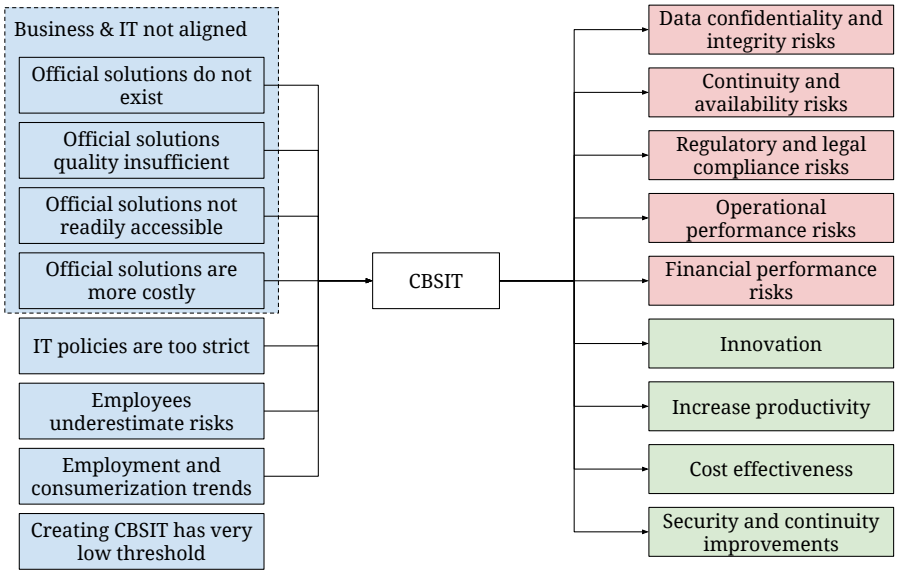

Figure 5.1: An overview of the categories of causes and effects found as an answer to Knowledge Question 1

categories. In many cases, the decision to "go rogue" is the result of a decision that weighs the cost of obtaining the means to do a job through official channels (which may include the official channel having to change what it offers) with the cost of making/buying it unofficially. In other words, transaction cost theory governs much of the Shadow IT domain [71, 14].

Lack of Business-IT-alignment

Almost all authors identify causes that boil down to employees turning to shadow IT based on the legitimate desire to do their job, and the enterprise not providing them the means to do so, implying that there is a lack of Business-IT Alignment (BITA). Several authors emphasize this classic root cause, which is found in an analysis of a wide variety of problems. King [38] points out a lack of communication between business units and IT departments. Smyth and Freeman [57] find that IT departments are often focused on their internal goals, and have little incentive to focus on requests from other departments. Behrens and Sedera [3] mention that development processes are often not transparent, leading to unmatched expectations. Even when trying to provide fitting services, IT departments offering technical services often do not fulfill functional requirements from users [57, 25]. This lack of communication leads to several types of mismatches between users and the IT providers in an organization, which in turn lead to a decision whether the cost of solving this alignment problem is lower than the cost to circumvent it. The following sections are in fact instances of this phenomenon.

Official solutions do not exist

The first and most intuitive form where a lack of BITA causes shadow IT adoption is when official solutions do not exist in the organization where users adopt shadow IT. For example, an organization may not provide image manipulation tools, causing a marketing department to obtain the software themselves. Other examples would include a sales application that is not available on mobile devices that salespeople carry with them, although it could be argued that this fits in the next category.

Furthermore, when talking to IT, employees who explicitly require the usage of a cloud solution often find that their IT department is unable to support the use of that application in an official capacity, according to Mann et al. [45]. Mann et al. find that IT departments are often unable to accommodate for the pace at which these services are developed and updated.

Even if the organization has a solution in place that would fulfill the needs of the employee, there is still a chance that employees resort to shadow IT if they don't know it exists.

Official solutions are of insufficient quality

It is hard to draw the border between the previous section and cases where official solutions that are of insufficient quality. Generally, in these cases the organization has a system, but users decide not to use it or to supplement

it because it does not fit with their needs. The system the organization provides may be badly adjusted to business processes as Behrens and Sedera [3] describe their example is a university ERP where looking up information on students required a multitude of steps in several official systems, whereas the shadow system facilitated this in a streamlined way. The system could also be slow or inaccurate or too general: Booz Allen Hamilton [6] gives the example of reports that can't be sufficiently customized. The opposite of a system that is too general also falls under this category: a virtualization environment that only allows Linux VM's while a Windows machine is needed. Again, one could argue that the last example falls under the previous category, as they are closely related.

Ky [43] argues that the superior usability and convenience that cloud based storage solutions brought in one of his case studies was an important reason for users to employ these solutions in lieu of official systems.

Official solutions are not readily accessible

Official solutions may also not be readily accessible. This may again seem like a similar problem to the causes mentioned above, but is quite distinct. In these cases a product or service that fulfills the requirements is provided through official channels, but for bureaucratic or practical reasons the access is limited. The resource may actually be limited, without budget for expansion, for example if a file server's disks are full and there is no possibility of adding more. Alternatively, the procedure to obtain resources may be complex or take so much time that alternatives are considered.
More even than with traditional shadow IT, cloud-based shadow IT is perceived as rapidly and easily deployable [26]. There is often little effort required to deploy a cloud solution, and virtually no time between the purchase and activation. The whole process can be done by any employee using a credit card, which circumvents delays through procurement and finance departments[18]. This further increases the perception that services provided by an IT department are too slow.

Official solutions are (perceived to be) more costly

The fact that official solutions, that are otherwise fitting and readily available, are (perceived to be) more costly is a fourth factor [6]. Sometimes this is the result of neglecting the costs of going rogue for other business units, including sunk costs for purchased infrastructure owned by an IT department. It could also be because solutions sanctioned by IT are subject to stricter requirements in terms of confidentiality, integrity and availability. Even after consideration the costs of shadow solutions may still be lower than opting for official solutions, while in other cases the consequences of taking a shortcut may manifest in any of the risks discussed in later sections[18]

As mentioned below, the capabilities to create shadow IT are a prerequisite for its deployment [23, 25]. Cloud based shadow IT greatly reduces the need for financial means to set up shadow systems: the pay-as-you-go-structure of cloud services also an attractive way of avoiding capital expendi-

ture [43]. Many services are even offered for free, albeit with limited capacity, capabilities or without a license for commercial use.

Employees underestimate risks

Related to this are the beliefs that employees have about the cost of security and compliance. Bulgurcu et al. [9] found that employees weigh the perceived cost of compliance, cost of noncompliance and the benefits of noncompliance (employing SIT). A lack of governance is related to these beliefs [6]: setting and enforcing policies and creating awareness is key in shaping the decisions users make after weighing the security and compliance impacts of their decisions to use shadow IT. Several sources also mention situation where technical (security) policies restricted users' work processes to the extent where they decided to obtain solutions not governed by these limitations [43, 60, 67]. Examples of a security policy is disabling USB storage devices to prevent data leaks. Another example is a policy of restricting the size of email attachments. Without an alternative, such restrictions could lead users to adopt other file sharing solutions (in this case a cloud storage platform) [43]. Haag [26] however, mentions that perceived security risks do not show significant effect in driving users away from cloud-based shadow IT. In addition, many users do not consider cloud solutions insecure, as they expect a level of expertise in securing such solutions from a CSP. In line with that, externalization of IT functions to either Managed Service Providers or Cloud Service providers further increase confidence in the use of systems that are provided by third parties [43].

Creating CBSIT has very low threshold

A prerequisite for the creation of any shadow system is the availability of the means to create a shadow system. These means consist of knowledge, available manpower and financial means. Shadow IT often required considerable expertise and upfront investment from a business unit to develop and maintain. Building a shadow system required knowledge of software engineering, and in some cases where shadow software was integrated into the organization's ERP system [2], knowledge of that system was required as well. Depending on the type of system, dedicated (server-)hardware could be required, or licenses need to be bought. Many of these hurdles have been taken away nowadays as cloud services can be purchased with a credit card, significantly lowering the bar[16, 11].

Employment and consumerization trends lower barriers

Finally, there are various lines of reasoning that are less motivated by financial, security and regulatory perspectives. These include employees using services that they are familiar with (which is a different factor from superior usability of shadow services), in lieu of learning to work with the alternatives the organization offers[43]. As the line between home and work shifts and blurs, employees are less keen to accept the difference in adoption speeds between the two environments.

There are various other factors that authors think contribute to the creation of CBSIT.

Ky [43] mentions that the usage of "cool" cloud services served as a "fashion icon" and were a way to derive status, an observation that King [38] adds to by saying that this "coolness" is partially due to the fact that the services are not sanctioned.

Ky [43] also invokes the concept of network externalities (as used by Shapiro and Varian. [54]), arguing that the incentive to use a shadow solution lies in the compatibility with other users who have installed it for personal use. This effect is strengthened by the blurring of the line between private and work life.

Without further explanation, Ky [43] also considers the average age of leadership as a high impact driver of cloud based shadow IT. This could be reasoned to impact many of the drivers mentioned above, and business-IT alignment in general.

Cause category	Found in
Business & IT are not aligned	[38, 57, 3, 63]
-Official solutions do not exist	[6, 23, 43, 60]
-Official solutions are of insufficient quality	[6, 3, 63]
-Official solutions are not readily accessible	[6, 3, 60, 62, 67]
-Official solutions are (perceived to be) more costly	[6, 23, 25, 53, 60, 62]
Employees think policies are too strict	[43, 60, 67]
Employees underestimate risks	[9, 26, 43]
Creating CBSIT has very low threshold	[2, 16, 11]
Employment and consumerization trends create opportunities	[43, 60, 38]

Table 5.1: Overview of causes of Shadow IT as identified in literature and interviews

5.2 EFFECTS

As in the previous section, the gathered selection of literature was searched for descriptions of effects of shadow IT. These were then grouped into eight categories of effects described by authors. Six of these categories indicated risks or otherwise adverse effects, while two of the categories indicate positive effects of shadow IT.

5.2.1 *Negative effects*

DATA CONFIDENTIALITY AND INTEGRITY RISKS

Smyth and Freeman [57] are some of the first authors to indicate potential security risks of shadow IT, citing that among the executives they surveyed,

it was the principal concern regarding shadow IT occurrences in their organizations.

D'Arcy [16] indicates that security risks can be caused by employee devices such as smartphones, tablets and storage media physically leaving the organization, contrary to fixed desktop PCs.

If not properly supported by an organizational Bring-your-own-Device (BYOD)-policy (which is the case with shadow IT) and device management, the organization also has no control over software that these devices run. This software may have inadequate security mechanisms, such as personal firewalls, or be improperly configured, e.g. weak passwords and accounts with elevated permissions. The devices may also be infected with malware as a result [60].

Combined with the fact that external networks such as mobile 3G/4G data networks and employees' home connections are not monitored and firewalled by corporate IT departments, data leaks over these networks are a risk.

The risks described go much further than devices that employees bring and install software on. If users purchase or develop (client-server) systems, virtualization environments and various other systems, they may not employ the same degree of protection that is incorporated in the enterprise's systems, such as in-transit and at-rest data encryption, or passwords with sufficient entropy and history requirements.

Another potential security risk mentioned by Stratecast | Frost & Sullivan [60] is the possibility of leaking passwords. A well designed system will have mechanisms such as strong hashing and salting of passwords stored, or connect to a system with such facilities (e.g. an enterprise's Active Directory server) for its authentication. A shadow system may store an independent set of username/ password-combinations which may be identical to the combination that users have set up for use in enterprise systems. Compromise of such a system means that enterprise systems are vulnerable to abuse.

Various authors discuss the security risks of individual employees or business units using cloud based shadow IT. In some cases, the risks they indicate are general to cloud computing projects that badly manage their risks, which is often also the case with CBSIT. For example, Haag [26] mentions the risk of exposing data to a multi-tenant-environment. Stratecast | Frost & Sullivan [60] finds that 37% of interview IT executives fear encrypted data will be susceptible to breach if placed in a shadow cloud solution, and that they are liable in case this happens. In the same study, an even higher percentage (42%) fears that user names and passwords of their employees are at risk if employees sign up for cloud based services.

Finally, many of the interviewed experts expressed concerns that data is placed in cloud service accounts owned by employees, which are outside of the enterprise's control. Upon termination, this information is still accessible to the employee, and the organization has no way of removing it[13].

Continuity and availability risks

Corporate IT often has stringent continuity-requirements. Specialized hardware and software are used to prevent outages due to hardware wear and tear or faults, and products are procured with a guarantee that they will be supported during an expected required life cycle. The markup in costs for these products is often steep, meaning it seems attractive to the creators of a shadow system to forego them altogether.

Although in practice not always complete and up to date, organizations also document various properties of their information systems in order to preserve that information in the case that knowledgeable personnel leaves their organization. Business units setting up shadow systems may not realize the value of such documentation or may not have the resources to set up a complete and up to date documentation of the solution they created. As a consequence, if the maintainer of a shadow system leaves the organization and the system breaks down, any processes or functions that have come to depend on it are also impaired.

Several experts stated in interviews that they were concerned about this effect occurring when an employee uses their personal account at a cloud service to support a process or as the sole storage point of critical data, and this employee leaves the organization. The organization is left with an impaired ability to support this process or without its critical data[18, 13]

Although, as discussed in a section below, a general characteristic of many cloud services is that their availability is above par, this does not count for all CSPs. Though the cost of outages can be mitigated by agreeing on a Service Level Agreement beforehand, shadow systems may not have been procured under such terms.

In addition to actual outages at the CSPs, as cloud-based shadow services are accessed via the internet, their adoption increases the reliance of employees on the availability of connectivity to that cloud service [60], which may be interrupted by the failure of the employee's internet connection or any intermediate networks.

Heath [28], Linthicum [44], Chan et al. [11] and several other authors point to the risk of vendor lock-in, if data is not available for download in a standardized format, or services that run on a cloud service cannot be modified to work on a competing platform. In that case, if a vendor terminates the service or employees would like to move to another service for different reasons, they find themselves unable to make that switch. That risk is real: a survey by Stratecast | Frost & Sullivan [60] finds that over 40% of surveyed IT executives fears that data may be lost or deleted by their provider.

Regulatory and legal compliance risks

Organizations with SIT may also face issues in demonstrating compliance to regulation. This is an issue that is quite often referred to in literature, although authors do not go into detail as to the nature of potential violations.

The regulations that organizations have to comply with differ by the jurisdiction they are in, and may complement or contradict if organizations operate in various geographies.

American organizations may face federal regulation such as the Sarbanes-Oxley act (SOx) of 2002[1], in addition to any state laws that apply. In Europe, regulation may stem from EU or national levels.

As such, providing a complete overview of infringements to regulations caused by SIT goes beyond the scope of this section. Two high level examples are control over data for financial reporting and requirements for processing Personally Identifiable Information.

SOx [1] requires that information in financial reports is traceable and verifiable, therefore requiring that the organization is in control of the systems that process this information and can ensure its integrity and accuracy. Any SIT that processes data and provide data used in reporting therefore potentially leaves the organization non-compliant with SOx.

On the other side of the Atlantic, the EU Data Protection Directive [20] and its intended successor, the General Data Protection Regulation, impose restrictions on the way organizations process information on natural persons. For example, it is expected that individuals would have the right to demand erasure of all data about them from an organization's information systems. Without control over which information systems are used to store various types of information, such a request is impossible to fulfill completely, leaving an organization non-compliant with EU law.

A characteristic of many cloud service providers is that they use multiple data centers around the world from which they provide their services. Although some are able to guarantee the location where data is stored and processed upon negotiation by the customer, it is possible that SIT may not be purchased under such conditions. As such, an organization using these services may be in violation of the EU's Data Protection Directive [20], which states that certain data is not to leave the EU if the receiving entity is unable to guarantee certain safeguards. Specific to the Netherlands, in effect since January 2016, is the new law governing mandatory reporting on data leaks ("Meldplicht Datalekken") [40].

Even if SIT does not directly cause non-compliance to regulation, the fact that it adds complexity to the IT landscape makes it more difficult to audit an organization's systems and state that it is in compliance with regulation.

In addition to regulatory compliance, organizations face legal risks, such as being held liable for employees' use of unlicensed or improperly licensed software. An employee who does not purchase a license for software he or she uses, but instead chooses to rely on an illegally obtained or cracked version exposes the organization he works for to the risk of litigation. The same goes for employees who, perhaps in good faith, use software whose license grants free use for personal purposes, but requires commercial licenses for commercial use.

Walters [65] states that the question of data ownership arises in a situation where employees choose to use certain cloud-based tools. They give

the example of an employee using social media using an account that was tied to him as a person. Upon his discharge, obtaining required information from that account proved difficult for the employer.

Another example would be a service that required, in its terms and conditions, users to surrender some or all rights to intellectual property and data they process using the service, or to provide a license for the service to use or resell intellectual property.

Operational performance risks

SIT may also hamper the ability of the IT department to supply technology that supports business processes, to operate this technology properly, and may thus hurt the execution of these business processes themselves. There are various reasons for this, having to do with limited insight in the bigger picture due to SIT solving local problems as Fuerstenau and Rothe [23] say, or lacking sufficient quality assurance in setup and changes

Organizations have formalized processes for various reasons. Best practices are implemented to increase productivity in addition to compliance purposes as discussed above. SIT that does not follow these processes may thus hamper both productivity and alignment in processes shared between departments with and without access to the shadow systems. Strong et al. [61] note the rigidity of an ERP system and the problems it causes when employees created workarounds, borrowing parts from different intermediate products to do their job of assembling another product, while keeping track of these parts unofficially. However, at some point such inventories need to be reconciled with the ERP system and mismatches between expected and current inventories do come to light.

Organizations with complex IT landscapes bring order to potential chaos by creating an enterprise architecture, a blue print of the systems, interconnections and dependencies supporting business functions and processes. Any changes made to the IT landscape can be checked with the enterprise architecture, and measures can be taken to ensure that the change does not have adverse effects on other systems. Shadow systems are not present in an enterprise architecture. This hinders the ability of IT to verify that a change in IT does not adversely affect business processes, as they may be supported by SIT outside their knowledge. It also means that IT is unable to verify that a change in a shadow system is without negative consequences for the rest of the IT landscape. A change in an official application's authentication mechanism may lead to a shadow system repeatedly attempting to authenticate itself, in essence performing a Denial-of-Service-attack on the enterprise's own systems.

SIT also has adverse effects on the support that an IT organization is able to provide to users of systems. Raden [53], Katz [36], Symantec [62] and Ky [43] all discuss the possibility that users working with a shadow system without knowing that it is one will demand some form of support from an IT support desk if they encounter problems. Not only does this directly increase the workload on support personnel, the problem is aggravated by the fact that

personnel is not prepared to provide support in the same way they would for official systems. At the same time, Smyth and Freeman [57] find a lack of support one of the main concerns over SIT, suggesting that organizations have little choice but to provide support wherever possible.

Finally, SIT may act as a barrier to the enhancement of both technology and operations. While official solutions can undergo planned maintenance or upgrades to align them with improved business processes or to increase the performance or security of the systems, the decentralized nature of SIT makes this more difficult. Raden [53] gives the example of employees using a set of spreadsheets that they email around as an example of SIT that is particularly difficult to upgrade. Changes in official systems may break compatibility with these spreadsheets, and the way they are spread makes it difficult to distribute an updated version. As such, any centrally decided improvements and innovations reach the organization less rapidly, or may altogether be postponed in order to not break compatibility.

Financial performance risks

Several authors discuss the impact that SIT can have on the financial side of IT operations. Gartner [24] predicted that by now, 35% of IT spending takes place outside control of the IT department. A recent survey by PWC [52] finds an even higher number with up to 47% of IT spending taking place outside the CIO's control.

Whether this is a problem in itself is up to debate, as King [38] cites research that implies correlation between an organization's performance in the digital domain, and a greater portion of IT spending taking place throughout the organization, indicating that technology is better interwoven in the organization's culture.

Elemans [19], Fuerstenau and Rothe [23], Gyoery et al. [25], Raden [53] and Symantec [62] mention a loss of synergy or economies of scale due to the repeated implementation of SIT in different business units.

In some cases, these are shadow systems that are redundant to each other, as various departments try to provide systems that fill gaps in the solutions provided by central IT. In other cases the shadow system is redundant to a centrally provided solution.

In both cases, expenditures are higher than necessary. Systems purchased separately do not offer a chance to obtain volume discounts for hardware or software licenses, meaning that more money is spent on assets. Other costs are the redundant work on installing and testing the system, and procuring training for small groups of users. Upon discovery of SIT and integration or elimination of these systems, a reduction in operational expenditure is still possible, but a large part of the capital expenditure is sunk[18]

The decentralized nature of control over SIT may also lead to the use of inconsistent business logic in making financial decisions. Different versions of spreadsheets floating around in an organization, or incorrect interpretation of the meaning of certain types of data by SIT could lead to unwanted decisions [53].

At the core of many cloud computing solutions is the pay-as-you-go-model. Advantageous in cases where capacity is suddenly needed or where a service is scaled down to reduce its cost, this model also reduces how predictable costs will be if demand cannot fully be predicted. If no agreements are made beforehand about placing a limit on costs incurred, various factors could cause costs to rise.

5.2.2 *Positive effects*

Increased productivity

While many authors stress the negative impact of SIT, some shed some light on the positive impact it has. Given that many of the causes identified in the previous section can ultimately be traced back to employees being unable to obtain tools to perform their tasks well enough, an obvious upside of SIT is that in some cases, the productivity of employees rises through a better fit between the task they are performing and the SIT supporting them in performing that task[43, 71]. Examples of this include systems for collaboration within the organization (because such tools were unavailable) or between organizations (because employees of both organizations use the same service in the form of SIT).

Productivity may also be increased because a shadow system that is being used in lieu of an official system has greater usability. Employees can therefore use time otherwise spent on training or becoming familiar with the official system for productive work [19].

Furthermore, the possibility for employees to determine for a large part which services they use to perform their tasks (e.g. SIT) affects several intrinsic motivators for employees and increases employee satisfaction [19, 43], thereby leading to increased productivity. Ky [43] and Raden [53] mention employees experiencing trust and autonomy as adding to their productivity, in addition to an increase in technical abilities.

Cost effectiveness

Another driver for creating SIT mentioned in a previous section was an estimate by employees that the SIT would cost less to set up and operate than the official alternative. As that section mentions, these estimates often neglect various factors such as sunk costs, quality factors and legal issues. However, even when these factors are considered, SIT may still be more cost effective.

As mentioned above, the reduced training time required to operate SIT that users are already familiar with, which is often the case given the trend of consumerization, adds to cost effectiveness.

Innovation

Being in contact with various forms of SIT may also improve the ability of an organization to innovate its technology. Keeping track of every new trend in a fast moving sector like IT is difficult, but required less dedicated effort if

initiatives from the entire organization are recognized [2, 25, 23]. Zejnilovic and Oliveira [70] find that of all innovations submitted by employees, those submitted by employee-users (i.e. those that are in use as SIT) have a significantly higher chance of getting adopted.

Security and Continuity Improvements

Contrary to the previous section on security effects, several authors and experts note improvements in both security and continuity are possible when employees switch to CBSIT [18].

First of all, cloud based solutions that replace traditional SIT bring the advantage that they are generally managed by a professional staff specialized in providing this service. Their security and continuity measures may well be better than those of an official solution [18]

Many cloud services offer some encryption at rest and in transit, enforce some password policies and have various other security measures implemented. In addition, many come with automatic redundancy, backup and revision history facilities, increasing both availability and the chance of recovering from accidental loss of data.

Even if SIT replaces an official solution, some organizations may still benefit [43]. For some organizations, the advantages outlined above go beyond what their own IT is able to offer.

Based on the above, the Cloud Security Alliance found that nearly 65% of IT leaders now consider cloud services more secure than their on-premise counterparts [15].

The section above, combined with the sections on data security and continuity risks, highlight a split between the security of the services themselves and the security which results from their proper use, as highlighted in the first validation interview.

Effect category	Found in
Data confidentiality and integrity risks	[57, 43, 60, 19, 25, 16]
Continuity and availability risks	[2, 25, 23, 43, 19, 57]
Regulatory and legal compliance risks	[2, 19, 25, 43, 53]
Operational performance risks	[19, 23, 57, 53, 25, 53, 2, 36, 43, 57]
Financial performance risks	[38, 23, 53, 19, 25, 62]
Innovation	[57, 2, 25, 23, 70, 63]
Increased productivity and satisfaction	[2, 25, 19, 43, 23, 53, 71, 63]
Cost Effectiveness	[43, 19]
Security and Continuity improvements	[43, 18]

Table 5.2: Overview of negative and positive effects of SIT as identified in literature and interviews

5.3 CHAPTER SUMMARY

This chapter has listed a variety of reasons why employees or departments choose to adopt SIT, and the myriad of consequences that this adoption can have. The diversity in cloud services that can be fielded as SIT also makes that reasons to use them as well as their effects are also diverse in nature, and when viewed at large, sometimes contradictory (e.g. CBSIT may cause IT costs to rise or drop, depending on the scenario). This chapter has therefore grouped the causes and effects in categories.

The causal categories show that a mismatch in communication, in understanding of costs and risks and in the supply-and-demand between business users and IT causes the adoption ofCBSIT, which is aided by the ease by which it is deployed.

The effects differ as well: some are largely based on risks that surround the implementation of any cloud solution, if that implementation is not done properly: risks surrounding compliance, confidentiality and continuity. Other risks are common to all forms of SIT: complex IT landscapes, redundant spending or spending outside IT budgets and availability risks.

At the same time, we see some advantages, since employees are able to quickly solve problems they encounter in their tasks by resorting to SIT they increase their productivity, reduce costs and provide a source of innovation.

The complexity, diversity and contradictory nature of all of the above also means that no simple solutions are available. Each organization studying the phenomenon of CBSIT should use the contents of this chapter as a starting point for its own analysis of causes and effects, in order to proceed with the next chapter: relevant measures to allow the organization to be in control.

6

METHODS FOR MANAGING CLOUD-BASED SHADOW IT

The second knowledge question introduced in chapter 3 investigates what organizations can do to manage CBSIT:

> KQ2: What are methods for managing Cloud-Based Shadow IT?

This chapter lists a collection of such measures, which are sorted into five steps of a process. The steps feature a Detection-Analysis-Response-process for dealing with individual CBSIT-services, combined with a prevention and evaluation phase, which aligns with in various works on (security) incident management [66, 35, 37], such as with the ITIL-cycle of incident management [42] , COBIT 5 [34], NIST 800-61[12] and ISO 27035 [33] as laid out in table 6.1.

1. Prevention - Prevent the creation of CBSIT.
2. Detection - Identify cloud services for analysis, either because they are in use or because they should otherwise be taken under consideration.
3. Analysis - Analyze what risks and benefits each service offers, and how that compares to the company's risk appetite.
4. Response - Choose, implement and operate measures to align actual usage with the chosen strategy.
5. Evaluation - On a regular basis, evaluate whether the chosen strategy and set of methods is still appropriate.

Process step	ITIL [42]	COBIT 5 [34]	NIST [12]	ISO 27035 [33]
Prevention	-	Planning and preparation	Preparation	Prepare
Detection	Incident identification	Detection	Detection	Identify
	Incident logging			
Analysis	Incident categorization	Triage	Analysis	Assess
	Initial diagnosis	Investigation		
	Incident prioritization	Analysis		
	Investigation and Diagnosis			
Response	Resolution and Recovery	Containment and recovery	Containment, Eradication and Recovery	Respond
Evaluation	Closure	Post-incident assessment	Post-Incident Activity	Learn
		Incident closure		

Table 6.1: Mapping of process steps to other frameworks

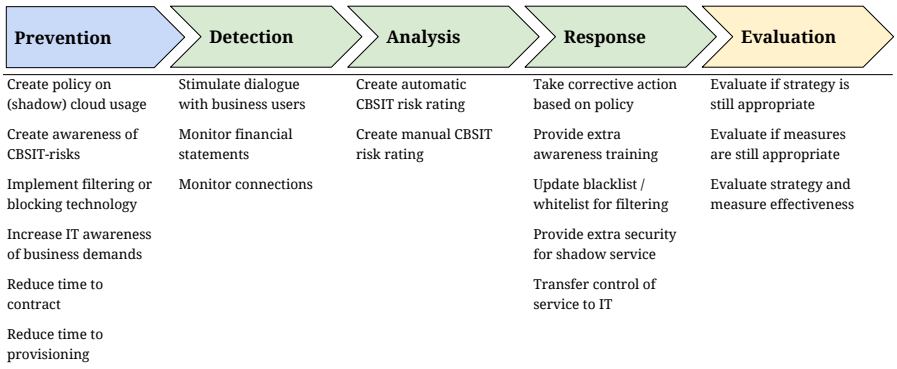

Figure 6.1: The measures discussed in this chapter

Figure 6.1 contains the measures explained in this chapter sorted by the two divisions explained above.

Finally, these measures are taken as the result of a choice to manage risks in a specific way. These risks have been identified in chapter 5, and table 6.3 at the end of this chapter gives an overview of how these measures impact both the risks and causes, while chapter 7 contains specific details per strategy, including how each measure is used for specific risks in every strategy.

6.1 PREVENTION

The measures in this section work by reducing the incentive for employees to resort to SIT, or by making it more difficult for them to do so.

6.1.1 *Create policy on (shadow) cloud usage*

An organization that wants to eliminate CBSIT should start by by putting in place policies outlining the organization's stance on CBSIT. If applicable, such policies should also state why the organization has taken this stance: which risks is it trying to mitigate, and why? This ties into the next section on creating awareness.

The degree to which organizations are able to impose sanctions upon an employee for violating this policy varies by the jurisdiction it is in, but may include termination, suspension and mandatory attendance of training.

As an alternative to a policy set and enforced without employee involvement, organizations may employ a code of conduct, which requires an employee to take note of and consent to rules regulating CBSIT[58].

Management buy-in and adherence to this policy is key for its adoption throughout the organization [30].

6.1.2 *Create awareness of CBSIT-risks*

One of the key factors determining whether employees decide to employ a cloud-based shadow service for any given task or type of data, according to both literature and expert interview, is their awareness of the risks it poses [10, CSC 17]

In order to influence their decisions, an organization can employ various measures to improve security awareness for individual employees. Examples include training, exams and certification. In addition to targeting individual employees, the organization can use periodic (i.e. campaigns) or continuous communications to all of its employees explaining their stance on cloud usage. As explained in the previous section, this communications should be backed up by, and include, official policies and the arguments for them.

Depending on the strategy the organization chooses, training can be aimed at goals other than deterrence as well. Thatte and Grainger [63] suggest the creation of Information Centers, where users of SIT can request support.

In the case of CBSIT, such centers could facilitate in selecting a CSP that meets the organization's criteria in addition to those of the user. It could also assist in safe operation of a cloud service, by assisting the user in setting up secure authentication (see section 6.6.2 and regular backups to prevent data loss at termination.

6.1.3 *Implement filtering or blocking technology*

In order to maintain control over employees' usage of cloud services, the organization can take a number of measures to prevent employees from accessing unwanted application functionality. This section explains some of the the methods to do that. Later sections will explain how detection, analysis and response to unwanted services may lead to changes in which services employees are prevented from accessing.

Several techniques exist to control employees' access to services. Simply said; these require filtering network traffic on the corporate network, controlling CBSIT usage from the device, or both.

The first technique, blocking connections at a gateway or a proprietary DNS service where the address of a cloud service is looked up, has the advantage of requiring no configuration at the individual devices that a user uses while that device is on the corporate network, and therefore configurations cannot be undone [49]. Solutions that filter connections using a proxy might require configuration of this proxy on every device, but by blocking all traffic that does not go through this proxy this solution ensures that, regardless of the specific configuration of the endpoint, no connections that are not allowed can be made from the corporate network.

In addition to simply blocking connections, some solutions allow more extensive control over connections to cloud services. For example, they may block access to only parts of services, to specific user accounts, filter the transmission of sensitive information or redirect the user to a sanctioned

alternative. As described in the section on monitoring, these more advanced methods of control require decryption of traffic, and more extensive control of the endpoint [50]

These method of blocking has the disadvantage that it does not work if the device is outside the corporate network and is otherwise connected to the internet. One expert argued that the share of such devices will grow in the next few years as the bandwidth of 3G and 4G services grows exponentially [18]. Implementations of this measure could include configuring devices exclusively for internet access through a Virtual Private Network (VPN) or enforcing the use of a proxy even outside the corporate network, although the advantage of not having to rely on the device's configuration no longer applies.

Connection blocking can also directly take place at the level of the individual device. Measures such as software firewalls, adding entries to a device's "Hosts file" or software security policies that forbid browsers to visit certain domains.

The advantage of this measure compared to blocking at a gateway or proxy is that it works even if the device is not routing its internet traffic through the corporate network directly or via a VPN.

The disadvantage is that it relies on the organization's ability to control the configuration of the device and its willingness to do so, thereby restricting the freedom of its employees to configure their device, which may inhibit productivity.

In addition to blocking certain services' traffic, any services that require the installation of software on a user's devices can be blocked. Although the majority of cloud services require no installation at all, or continue to work with limited functionality, services such as Dropbox rely on a local client to provide their core functionality.

Mobile Device Management solutions for mobile phones and tablets allow administrators to block installation of specific apps beforehand, while such measures for laptops and desktops with a different operating system and different application ecosystem generally block software installation as a whole (by not granting users local administrator rights and blocking the execution of unchecked code) or perform regular scans identifying software on a blacklist which is then removed.

6.1.4 *Increase IT awareness of business user demands*

Together with the next two measures, creating improved awareness of the demands of users takes away the grounds for employee adoption of CBSIT. Depending on the strategy chosen, there could be an active search for new services that could improve productivity, or a response to measured user demand. For example, if the detection phase shows a large demand for a specific category of services, the usage of such services as CBSIT could have been prevented if the organization had supplied a similar service.

6.1.5 *Reduce time to contract/implementation time for official services*

Another driver seen in chapter 5 was the fact that organizations often don't supply tools of the same functionality and quality that are available as cloud services on the market. Services such as personal cloud storage and collaboration tools are examples of such tools according to Ky [43] and interviewed experts.

In order to eliminate this driver, organizations' IT departments need be able to adjust their service catalog to business demands more rapidly. Depending on the reason why that is currently not the case, different changes need to be implemented. Examples are: increased staffing, a change in working methodology (from waterfall to incremental delivery) or the implementation of a two-speed architecture where traditional back-end processes are decoupled from more rapidly developed front-end applications[8, 7].

6.1.6 *Reduce time to provisioning for official services*

As one of the drivers of CBSIT identified in chapter 5 was the time it took for the IT department to fulfill a request to provide an existing service to a user, reducing that time reduces employees' need to use CBSIT. This could mean that procedures for obtaining resources are simplified, or that organizations need to ensure that they are executed with fewer delays. If waiting occurs due to capacity shortages, addressing those would reduce incentives for employees to resort to CBSIT.

6.2 DETECTION

6.2.1 *Stimulate dialogue with business users*

One of the most straightforward ways of detecting any form of SITis simply getting employees to tell the IT department what they are using [29]. Former Chief Information Security Officer for an intergovernmental organization [22] and other interviewed experts argue that in order to achieve a culture where that occurs, it is essential that IT responds to the discovery of SIT in a constructive way. Thus, the user should not be negatively influenced by his disclosure, for example by punishment or the elimination of the SIT he discloses. Thatte and Grainger [63] suggests the creation of information centers, which would advice users on a choice of safe cloud services, an approach that was endorsed in expert interviews[32].

6.2.2 *Monitor financial statements*

Christopher Null [47] proposes to turn one of the drivers of CBSIT against it. The appeal of using cloud services as SIT, is that even services that are not free only require a credit card for payment. Although this circumvents lengthy IT approval and procurement processes, it means billing transac-

tions from CSPs will appear on credit cards issued to employees or departments.

Alternatively, if payments are made through other means than credit cards, these payments can be examined as well as the payment must leave a paper trail. Any unpaid services used go unnoticed by this detection method.

6.2.3 *Monitor connections*

A very basic measure in order to detect what degree of CBSIT is in use in an organization is analysis of internet traffic. In order to do so, some way of measuring the volume and direction of traffic is required. In many organizations, internet traffic is directed via one or more gateway or proxy servers. These servers can be configure to log several data points for each established connection, such as the clientś internal network address, the address and port number of the service and the volume of data sent and received.

Automated solutions exist to analyze these log files, and determine whether a given a flow of traffic connects to a cloud service [10, CSC. 7.4]. Somewhat more advanced systems may perform this analysis in real time, allowing it to send alerts and allowing the organization to respond quickly.

Even more advanced systems are capable of providing insight into the contents of the communication. As communication to and from cloud services is generally encrypted, this is impossible without additional measures. Some firewalls allow for the inspection of encrypted of traffic in real time, thus allowing it to inspect more precisely what the user is doing. Depending on the jurisdiction that the organization operates in, this may be unlawful. In addition, it requires control over the user's endpoint as a certificate needs to be installed on the endpoint. The user's endpoint then encrypts its connection to the firewall/proxy only, after which the latter sets up an encrypted connection to the cloud service. This creates a decrypted view for the firewall/proxy, allowing it to filter data directly or offer it for analysis to a third party service [50].

There are also other technologies available, such as configuring devices to use specialized Domain Name System (DNS)-servers that log requests for the Internet Protocol (IP)-address of a cloud service.

6.3 ANALYSIS

6.3.1 *Create automatic CBSIT risk rating*

If the services mentioned in section 6.2.3 are performed by tooling such as a CASB (see section 6.6.1), they go further than simply analyzing log files to identify services. They enhance this basic information with an assessment of the risk that the cloud service introduces, rating several aspects such as data leakage, data location, intellectual property rights and malware. Many of these products have databases containing tens of thousands of cloud services, rated on dozens of factors. They may allow adjustment of the weighing of

these different factors and the creations of rules to allow organizations to tailor the risk rating for the needs of the organization.

Despite this tailoring, such risk analyses are based on generic input and created for a vast array of services. They will therefore be less precise than an analysis of specific services for a specific organization. However, due to the relatively low cost of such an analysis they provide a useful starting point for a more in depth analysis of key services.

6.3.2 *Create manual CBSIT risk rating*

Given that an organization knows what CBSIT instances are in use and for which functions and processes they are used, the organization can base further actions it wants to take on a classification of the services in different categories. Bellino et al. [4] suggest a rating system for services that deal with financial reporting in their report on General Technology Audit Guidelines for the Institute of Internal Auditors. It consists of several factors to be rated per application:

- Financial Materiality: The value that the application reports on, both in terms of income statements and balance statements;
- Operational Materiality: The degree to which the application is relied on for operational processes;
- Compliance Materiality: The degree to which the application is used in reporting for compliance reasons;
- Risk Ranking: For the three options above, the impact and likelihood of risks caused by the application. Both are rated on a scale of 0-3, with a ranking score obtained by multiplying the two.

At a much higher level, the guideline recommends grouping based on business processes, where attention should be focused on SIT supporting more sensitive business processes.

Zimmermann et al. [72] also have a method of classification intended to separate SIT found in an organization into groups that receive different treatment: they propose to rate services in terms of their quality, as well as their criticality and relevance to business processes. Their ratings are then plotted on a graph (see figure 6.2, showing which action is to be taken. Although the actions proposed in the original paper are mostly for traditional SIT, the action categories map onto the measures from the next section.

In this figure, the RENOVATION section is for tools whose continued existence in that form poses a significant risk for the organization. For CBSIT his would map to blocking the application or part of its functionality, and possibly suggesting an alternative.

COORDINATION then maps to transferring the application to the IT department, and potentially securing its use by enforcing encryption, enforcing au-

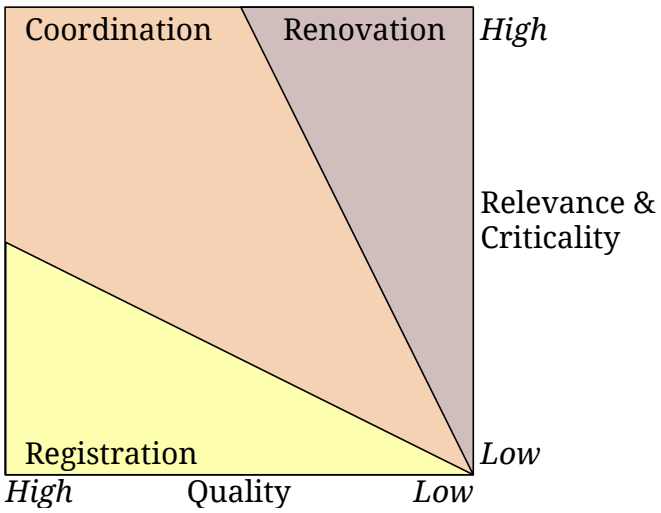

Figure 6.2: Shadow IT portfolio plot by Zimmermann et al. [72]

thentication with corporate credentials as well as any other measures that improve the tool in its current form.

Finally, REGISTRATION would be just that: registering the existence, purpose and risk rating of an application, and monitoring its use without taking an action influence it.

6.4 RESPONSE

6.4.1 *Corrective action based on policy*

If the use of an application is in violation of the policies intended to prevent CBSIT, the response could include taking actions against the violators. The exact nature of this response depends on the policy in place and the legal jurisdiction the organization operates in.

6.4.2 *Provide extra awareness training*

In complement to the general security awareness programs from section 6.1.2, the actions from the section above could also include additional training or awareness programs. As the "Prevention"-section on security awareness states, there are various things organizations would want to achieve with such training, depending on the strategy they choose and other factors. Both reducing the likelihood that the employee will adopt CBSIT, and increasing the likelihood that they will pay additional attention to risks when next selecting CBSIT are examples of goals.

6.4.3 *Update black/whitelist*

If the organization has a blacklist or whitelist as indicated in section 6.1.3, the outcome of the analysis-phase may lead to the inclusion of an application on a blacklist, in order to prevent employees from accessing it again, or to inclusion on a whitelist, achieving just the opposite.

6.4.4 *Transfer control of service to IT*

A solution for managing traditional SIT, mentioned by Zimmermann et al. [72], is also applicable to CBSIT. As it is mentioned in the first interview, an organization can offer it's employees the opportunity to present the cloud services they use and have come to rely on to IT. The IT department takes over (part of) the payment for the service, in addition to the management.

This directly resolves the amount of spending on IT services outside the CIO's control, by placing spending that already takes place at the right place in the organization. It resolves issues with ownership and responsibility for securing the service, and allows the IT department greater control over integrating the service in their IT landscape [18]

If the same cloud service is indeed used in multiple places in the organization in an independent way, consolidating spending at the IT department allows for more efficient procurement for which the savings can be passed on to the business units. Discounts create an incentive for business units to take part in such a transfer.

6.4.5 *Provide extra security for CBSIT*

Instead of transferring the service to IT as it is or consolidating multiple (instances of) services into one under the control of IT, the service may be retained in a modified form with additional security controls in place. Examples of includes enforcing encryption or authentication policies when the application is used. Several interviewees mentioned this as a preferred method of treating CBSIT, with great added value if such a security 'layer' could be defined for various services at once.

6.5 EVALUATION

Organizations should regularly evaluate their approach to CBSIT for both appropriateness and effectiveness.

6.5.1 *Evaluate if strategy and measures are still appropriate*

As a first evaluation, organizations should periodically evaluate whether the strategy they chose, and and the measures that they took as a consequence of that strategy, are still appropriate. Although this can greatly be helped by

adequate reporting from a monitoring measure in order to see the amount of CBSIT present in the organization, it also requires more fundamental evaluation of the applicability of the various risk to the organization and the risk appetite of the organization in order to evaluate the requirements. At the same time, between these periodic evaluations, the means of the organization may have shifted so that more (or fewer) resources are available, more or less management sponsorship is available, the organization itself has changed or other reasons exist to revisit the choice of strategy.

Several of the validation interviewees mentioned that their current efforts may not have been optimal, but no priority was given the management of CBSIT. They did envision this changing in the coming period, therefore warranting periodically revisiting the issue [30, 13].

6.5.2 *Evaluate if strategy and measure are effective*

A periodical evaluation of the effectiveness of the strategy and measures an organization has implemented are required to see if they provide an operational fit with the organization. Regular, automatic reporting (i.e. dashboards) would provide better situational awareness [30].Having better insight in usage patterns, and thus demand, directly feeds back into measures aligning the IT service supply with demand (if the functionality is not yet offered) or better blocking rules and communication strategies (if the functionality of the SIT is redundant with that of a sanctioned alternative). Short cycles give unwanted CBSIT less chance to take root in the organization [30].

In general, evaluating the response measures is easy in the sense that all occurrences where a response is warranted are known, and thus can be evaluated.

Evaluation whether the detection mechanisms are effective is more difficult: how does one measure what one can't see? Having multiple measures working to the same effect may help: false negatives in one measure are picked up in another (e.g. finding a payment for a service that a connection monitoring solution has not picked up).

Since the exact nature of the evaluation depends on the strategy chosen and the organization, this section is expanded in chapter 7

6.6 COMMERCIAL PRODUCTS

The measures identified above are described somewhat abstract and in a way that is agnostic of the way commercially available products have implemented them, in order to keep this research relevant as market offerings progress.

However, since the problem of CBSIT has existed for some time, market players have developed solutions that intend to cover several of these measures. This chapter explains two important ones: Cloud Access Security Brokers (CASBs) and Identity&Access-Management-as-a-Service (IAMaaS)-solutions.

6.6.1 *Cloud Access Security Broker*

Several market parties have developed products that help in identifying, analyzing and responding to traffic to and from CSPs. These products, aimed at securing an organization's use of cloud computing, are known as Cloud Access Security Brokers (CASBs) by the majority of the market, with some parties using the term Cloud Data Protection (CDP) solutions.

CASBs may offer the kind of detection using either traffic analysis or log file analysis, using a database to compare characteristics of internet traffic (such as the destination host) to determine whether traffic flows go to a specific cloud service. They frequently leverage that database to offer an automatic analysis of that cloud tool's usage to present organization's with several properties and metrics of that cloud service, such as the nature of the service, security aspects and an analysis of its terms and conditions. Combined with traffic properties such as the number of users and the amount of data flowing to and from that service this allows for an initial overview of an organization's risk stemming from CBSIT.

CASBs then offer responsive measures. They may offer blocking functionality, redirect users to a different service or add functionality to the cloud service that mitigates part of the risks posed by that specific cloud service, such as scanning for Personally Identifiable Information (PII), Protected Health Information (PHI) and Payment Card Information (PCI) and other Data Leakage Prevention (DLP) functionality.

As these products vary in their exact functionality, architecture and methods of integrating with an organization's current IT-landscape, an exact analysis of the products on the market would fall outside the scope of this thesis. This section aims to describe some of the key functions and characteristics of the products that comprise the majority of the market.

Integration technologies

The first distinction to be made between the various CASB-products on the market is the way in which they integrate themselves into the organization's technology. The sections below outline three main integration methods, while figure 6.2 shows how these methods can be applied to provide control in case of different categories of devices, networks and services.

FORWARD PROXIES require that the end user's device channels all traffic it generates through the proxy. On an organization's network, this if often done by blocking internet access to all devices except this proxy. For this to work outside an organization's network, additional controls on the user's device are required.

REVERSE PROXIES instead rely on the cloud service to redirect traffic from an organization's users trough the proxy, based on the user's credentials and a rule in the cloud service requiring users with those credentials to be redirected through the proxy.

API-INTEGRATION does not handle traffic like the methods described above, instead relying on the CSP's Application Programming Interface (API) to expose mechanisms by which the CASB can provide extra security controls, without requiring measures at the user's side. In order to make this work, the application has to be configured for use by the CASB, and the user must be recognized as a user from an organization, e.g. by signing in with corporate credentials.

Device on corporate network	Managed device	Sanctioned application/ IAMaaS sign in		Forward proxy	Reverse proxy	API integration
Yes	Yes	Yes	→	Yes	Yes	Yes
Yes	Yes	No	→	Yes	No (3)	No (3)
Yes	No	Yes	→	Yes	Yes	Yes
Yes	No	No	→	Yes	No	No
No	Yes	Yes	→	Yes (1)	Yes	Yes
No	Yes	No	→	Yes (1)	No (3)	No (3)
No	No	Yes	→	Yes (2)	Yes	Yes
No	No	No	→	No	No	No

(1) Always force VPN usage through device management
(2) Configure cloud application to only allow access access to forward proxy IP address
(3) This document assumes a light presence on the device, e.g. no full list of cloud applications and software to manage their connections and functionality locally

Allows management of the application
Does not allow management of the application

Table 6.2: Different scenario's where control is required and the applicable CASB integration methods.

Service location

An important distinction between several offerings of CASB-providers is the location of the service. All of the connection mechanisms from the previous section can be on the premise of the supplier (typically as a cloud solution), or on the premise of an organization: typically as a virtual or physical appliance which then either integrates with the organization's existing proxy or functions as proxy appliance in itself.

If the service is provided off-premise, organizations using the service should verify the location of that service as being inside or outside specific data processing jurisdictions (e.g. outside the EU, but processing data on EU citizens. If the latter is the case, the organization should verify that moving the processing of web traffic outside their data processing jurisdiction is allowed.

6.6.2 *Identity & Access Management as a Service*

Analogous to developments such as BYOD, where organizations adapted their infrastructure to accommodate a wide variety of devices in a secure way, organizations can adapt their infrastructure to reduce some of the risks that CBSIT brings.

An organization could provide the means to use the organization's authentication facilities as a mechanism for authentication to cloud services. This concept is covered to a limited extent in literature, but was mentioned

by several of the interviewed experts as a way of limiting the risks that are associated with users using their own credentials, as described in chapter 5.

Standards such as Security Assertion Markup Language (SAML) [27], OAuth[48] (Open Authentication) or OpenID [64] allow third party CSPs to leverage the organization's authentication mechanisms to identify users of their cloud services without the need for users to create a separate account. For users, this is easier because they don't need to go through the hassle of creating and maintaining an additional set of credentials. For organizations, this offers the opportunity to centrally manage some entitlements for cloud services, including the option to terminate access to third party services that an employee used for work upon the discharge of this employee. It also reduces the likelihood of users entering the same credentials they use for authentication within the organization as the credentials for third party services.

Alternatively, providers of IAMaaS offer a more limited form of authentication for pre-approved services only. While this will not mitigate risks associated with users re-using credentials or an inability to remove their access to services upon termination, it makes it easier to facilitate official implementation of cloud services, reducing implementation time and potentially eliminating the need for SIT from a user's perspective.

While not a full-featured IAMaaS-solution, and not intended as such, services such as Google Apps for Work and it's cloud based directory structure can be used in part to provide an organization's users with the possibility to use their organization's credentials to sign in on any cloud services that offers to "Sign in with Google".

6.7 CHAPTER SUMMARY

This chapter, at the start, set out to answer the second research question.

KQ2: What are methods for managing Cloud-Based Shadow IT?

In order to do so, the first section introduced a five step process in which the measures were presented in a structured way, combined with two market solutions to support various measures.

The five step program intends first to prevent CBSIT by both introducing measures to eliminate the need for employees to adopt it, and to take away the opportunity to do so.

It then introduces a step containing detection measures to find any instances of CBSIT, followed by a step containing measures to analyze these services for their risks and benefits, and a step containing various responses to be taken based on that analysis.

Finally, this chapter introduces an evaluation step, which evaluates both applicability (are we doing the right things?) and effectiveness (are we doing things right?) of the measures and strategy the organization chose and implemented.

An overview of the steps and their measures is in figure 6.1, while table 6.3 shows the impact on causes and effects of CBSIT

	Prevention						*Detection*			*Analysis*		*Response*					*Evaluate*	
	Create policy on CBSIT	Security awareness training	Implement connection filtering technology	Improve awareness of business demand	Reduce time to provisioning	Reduce time to Contract	Employee disclosure	Examine expenditures	Connection logging	Manual classification	Automatic classification	Corrective action based on policy	Provide extra security awareness traning	Update blacklist / whitelist for filtering	Provide extra security for CBSIT	Transfer of solution to IT	Evaluate appropriateness	Evaluate effectiveness
Causes																		
Business & IT are not aligned				X														
Official solutions do not exist				X		X												
Official solutions are of insufficient quality				X														
Official solutions are not readily accessible					X													
Official solutions are more costly				X														
Employees think policies are too strict				X														
Employees underestimate risks	X	X										X	X					
Employment and consumerization trends				X														
Effects																		
Data confidentiality and integrity risks	X	X	X	X	X	X								X	X	X		
Continuity and availability risks	X	X	X	X	X	X								X	X	X		
Regulatory Compliance risks	X	X	X	X	X	X	X	X	X	X	X			X	X	X		
Operational performance risks	X	X	X	X	X	X	X	X	X					X		X		
Financial performance risks	X	X	X	X	X	X		X						X		X		

Table 6.3: An overview of how both causes and effects of CBSIT are impacted by the measures proposed in this chapter

7 STRATEGIES REGARDING CLOUD-BASED SHADOW IT

The third and final knowledge question investigates how organizations could approach cloud based shadow IT in a coherent manner:

> KQ3: What are possible strategies regarding Cloud-Based Shadow IT and how can they incorporate the measures (from Question 2)?

Literature on SIT predominantly describes the traditional form where IT administrators encountered a single large instance of a shadow systems, and rarely considered proposing strategies as a conscious choice that would set the baseline for future occurrences of SIT. Thus, many articles described ad-hoc treatments.

As such, the strategies in this thesis were based on interviews with experts and formed in discussions with various people during the research. They are based on general principles of decision making in other contexts where some form of filtering is relevant.

In the end, the strategies emerged as outlined in figure 7.1. These strategies represent a spectrum ranging from totally ignoring or fully allowing any CBSIT to attempting to block every unsanctioned cloud service. The following sections explore these strategies in some more detail.

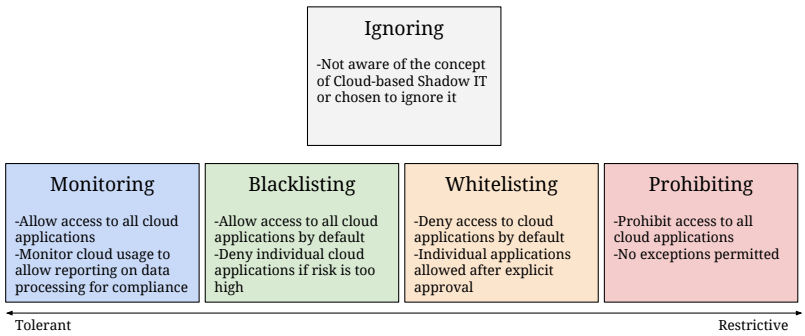

Figure 7.1: The five strategies explained in this chapter

The step of defining the strategies and the measures that are relevant to them, the framework takes shape, as can be seen in figure 7.2.

7.1 IGNORING

Many organizations are unaware of the concept of SIT and associated risks, and therefore have not made a choice for a strategy, ignoring the concept as a consequence.

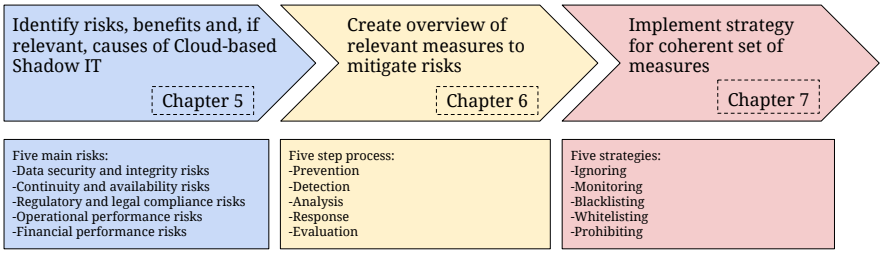

Figure 7.2: Overview of the framework

For other organizations the cost of actively managing or even monitoring CBSIT through technical means is disproportionately high, budget is not available, measures would interfere with or hamper important processes or there is very little risk of leakage of Intellectual Property or sensitive data. These organizations may consciously opt to ignore the phenomenon of CBSIT.

Since this decision means that they will not take any measures, this chapter will not further explore this strategy.

7.2 MONITORING

Organizations following this strategy will monitor cloud services in use. This provides them with information required for compliance with certain laws and regulations on where and by whom their data is processed.

They also gather information about the needs of their employees through the usage patterns they detect, and they can try to formalize existing tools or provide enterprise alternatives in order to eliminate some of the downsides that shadow solutions bring, particularly in terms of duplicate or misallocated costs and lack of synergy. Additionally, monitoring the organization's use of CBSIT allows for periodic checks whether a switch of strategy is warranted.

7.2.1 *Prevention*

Since this strategy limits does not block applications, pushing them towards sanctioned alternatives, getting employees to refrain from adopting CBSIT requires "pull". Measures should include improving their security awareness, aimed at making employees choose to use the sanctioned applications, or choosing services in such a way that they do not unnecessarily contribute to the set of risks associated with CBSIT. At the same time, organizations should focus on the measures that improve both the services that their IT department offers, and the way these are offered. They should better align their portfolio with demands, and reduce the time required to provision various services where no technical limitations exist and delays are primarily bureaucratic. This reduces the need for CBSIT, thus pulling employees towards the sanctioned options.

7.2.2 *Detection*

For detecting CBSIT, these organizations can use any of the measures introduced in the previous chapter. However, as there may be no current proxy or gateway present in the organization and since there is no intention to block the usage of any services, implementing one of these solutions can be too costly for the purpose of monitoring alone. Organizations following this strategy should consider a Cloud Access Security Broker (CASB) based on a subscription model, using limited functionality, DNS-based monitoring or, if a limited degree of visibility is accepted, one of the non technical monitoring methods.

7.2.3 *Analysis*

In order to quickly gain an overview of the usage of CBSIT in the organization, using some form of automated analysis of internet connection logs can be used. Although payment is usually required for the usage of these tools and the information they use to perform the analysis, they require limited human effort in analyzing any given application. As CBSIT is unrestricted in this strategy, the total number of services to be analyzed is likely to be large and diverse.

Based on the result of automated analysis, such as large volume of of data transferred to high-risk services, or interesting findings from financial analysis or users' suggestions, some further analysis can be performed. Using the methods from section 6.3.2, the organization should determine whether further action is warranted. However, as there is limited perspective for follow up measures, the cost of doing this should be kept low.

7.2.4 *Response*

Organizations following this strategy have limited their response measures, since they have excluded the option to block services they consider risky. Nevertheless, they have several measures at their disposal. By transferring control of the shadow solution to the IT department, and offering users an incentive to agree to this transition, they are able to control more of the aspects of the application, reduce double and out-of-place spending and potentially increase synergies by transferring multiple similar solutions. For this strategy in specific, organizations should keep in mind that they can only "pull" users towards the IT-managed services since the "push", otherwise achieved by blocking or restricting access to non-sanctioned services is absent in this strategy.

Using a CASB that integrates into a wide spectrum of cloud services, combined with a method of authentication such as an IAMaaS-solution, to enhance the security of services outside the control of IT is another method that is particularly useful in a strategy where limited levels of control/restriction requires that IT departments make it as easy as possible for users

to work with the security measures that the organization offers them, despite having the option not to do so.

7.2.5 *Evaluation*

Organizations that have a Monitoring strategy in place will most likely use the evaluation phase to see whether it is required to scale up their efforts to one of the three more strict strategies: Blacklisting, Whitelisting or Prohibiting. As a basis, they can take an evaluation of whether any measures they take to better align the organization's service offering with the demand of users is proving effective in reducing the amount of CBSIT, if that is a KPI by which they score the success of their measures.

In addition to an evaluation of strategy, if the organization has chosen to employ other response measures, such as securing services or providing single sign on, it can test whether these measures have the desired effect on shadow cloud usage.

7.3 BLACKLISTING

As several authors and interviewees describe the positive consequences of Cloud-Based Shadow IT (CBSIT) IT, an organization can employ their employees' individual deployment of cloud tools as a way to learn, test and innovate with cloud services to complement their central IT.

At the same time, cloud service usage is monitored. Any service that is detected is assessed, and if it is deemed to pose an excessive risk, its use is prohibited and users are required to use a different service.

Since new cloud services are launched every day, this strategy requires more effort than the other strategies, as continuous effort is required to stay up to date on both assessing newly found services and making sure that previously blocked services are still blocked in an effective manner.

7.3.1 *Prevention*

As in the previous strategy, prevention measures aimed at reducing the need for employees to create shadow IT can serve as a way to reduce some of the risks associated with shadow IT. However, as the strategy's name implies, the organization works with a blacklist of services of which the use should be prevented.

In order to do so, the organization should have a policy that explains both which services are blacklisted, what criteria are on which services are rated and why those are used, explaining why is is important for the organization to mitigate risks.

At the same time, the organization needs technical measures to block the use of blacklisted services, meaning that traffic should be routed through a firewall, proxy or other filtering device that is kept up to date with the blacklist.

7.3.2 *Detection*

The most important measure for detecting CBSIT in this strategy is the monitoring of connection to cloud services. Given that a key element of this strategy is the ability to block selected services, some form of centralized control over which connections are made should be present, meaning that the cost of fully automated detection is relatively low. To complement the information found by monitoring connections to cloud services (which is generally limited to the amount of data transferred), interviews with heavy users of shadow services can bring further insight for the analysis phase.

7.3.3 *Analysis*

Similar to the previous strategy, the large volume of data resulting from monitoring the use of unrestricted CBSIT is initially best analyzed in an automated way.

If a service is labeled as a high risk service in categories the organization finds relevant, if there are unusually large volumes of data or large numbers of users for a service or there are other indicators that the service requires further study, the methods mentioned in section 6.3.2 offer a first step.

7.3.4 *Response*

As the name of this strategy suggests, blocking cloud services in this strategy is done on a blacklisting basis. If the organization's analysis, such as in the previous step, indicates that a cloud service should not be used, it can create rules in its proxy or firewall that block connections to this service. It can also configure the software on the devices that employees use to be unable to connect to the service and to remove any installed software that the cloud service may require.

Depending on the service that is used to block a cloud application, several intermediate options may also exist. CASBs offer functionality to restrict access to certain functions of cloud services, depending on the CSP. For example, one vendor mentioned WeTransfer: a service where users can upload a large file, after which a download link is emailed to a recipient. The vendor's CASB could be set up to allow downloading files from this service, while blocking the uploading of files. This mitigates data leakage risks, while allowing people outside the organization to send users files without restriction.

Special attention should be paid in this strategy to the consequences of any action that is taken to block a specific shadow cloud service. Any service that is blocked may cause users to divert to other services, perhaps with even greater risks attached.

An example of such a service that is proliferate is Dropbox, a service that synchronized files between devices, and offers access to a copy stored on its servers via a website.

Although the service is considered by several interviewees to pose some degree of risk due to it data location, data retention and intellectual property policies, all interviewees agreed that blocking this service, which is among the most well known of its kind, might result in users choosing alternative services which may pose even greater risks. Interviewees and other experts expressed concerns about Chinese or Russian services [21, 22], such as Baidu or Yandex. It may therefore be a good practice to consider such alternatives even before their usage is detected and consider whether they pose a risk. If so, the organization can reconsider blocking the service, it can consider blocking these alternative services as well (redoing this analysis for each of them), or invest in offering a trusted alternative.

Although a shadow service may pose a risk that an organization is not willing to take which requires it to be blacklisting, its existence proves that there is a demand for it, thus simply blocking a service that is in demand may actually increase overall risks.

One of the options considered as an outcome of a shadow system's analysis as proposed by Zimmermann et al. [72] is to transfer the service to the IT department.

Depending on the exact nature of the service, this transfer can be executed in a different manner.

First, the service may be transferred as-is, thus primarily moving the location of spending and maintenance back to the IT department and mitigating these risks. Second, the service may be procured by the IT department in a modified form. An example of this is procuring an enterprise plan from a cloud storage provider to allow employees to use this instead of individually created accounts. Third, the organization may choose to offer a different service altogether. If the shadow IT landscape consists of a myriad of tools with a similar purpose, this option is in some way almost inevitable as the IT department would otherwise commit to a largely redundant effort.

7.3.5 *Evaluation*

In the Blacklisting strategy, the evaluation will often focus on the effectiveness of the measure by the same name; thus evaluating whether or not the blacklist of services leads to a reduction in risk from cloud shadow services.

The evaluation of the effectiveness of the blacklist can then lead to two things: a stricter implementation of the blacklist, with more technologically advanced blocking mechanisms or better information on how to filter connections to them, a wider array of blocked services (e.g. blocking known alternatives to a blacklisted service).

In addition to assessing the effectiveness of measures, the appropriateness can be assessed as well. Specific to blacklisting and whitelisting strategies, assessing whether the inclusion of a service on these lists is still appropriate should regularly occur, as cloud services may change, thus changing the risks they expose the organization to.

Finally, evaluation of the the appropriateness of the strategy could resulting in a switch to a whitelisting strategy where there is more control over which services are used.

7.4 WHITELISTING

The third strategy follows an opposite pattern compared to the first one. Here, an organization would attempt to eliminate shadow IT entirely. Instead of giving users some degree of freedom to experiment, the usage of unknown cloud services is prohibited by policies and technology, and this is communicated as such.

Users are, however, able to request permission to use a service. The service is assessed, and if it is deemed to meet certain requirements and does not pose an excessive risk, it is unblocked. Although the service is then not provided or contracted by the IT department, it also no longer meets the definition of being Shadow IT, since it's use is explicitly acknowledged and sanctioned by IT.

7.4.1 *Prevention*

The key to this strategy lies in a strong prevention implementation: if shadow IT usage is not prevented here, it is unlikely to then be detected, analyzed and responded to in a timely fashion to prevent the risks that the organization wanted to avoid from occurring. It is essential that this prevention is driven by people, process and technology measures.

First of all, it is essential that the organization has an adequate policy against the use of unsanctioned cloud services, and that it educates its employees to improve security awareness of why such a policy exists. It should stress, towards its employees, why the nature of the organization leads to increased efforts to mitigate risks from CBSIT, and back these statements up by providing clear consequences for violating the policy of not allowing CBSIT.

Following from a mandate set in the policies, technical measures that block access to non-whitelisted services and control traffic to whitelisted ones, Following from table 6.2, technical measures to control access to services have limitations that result from the organization managing either the network a device is on, the device that is used to access that application or the application itself. This means that

At the same time, since this policy does allow employees to request specific services to be green-lighted for use, the organization should support its employees in this process, ensuring the benefits of these user-chosen services arrive at their employees with minimal risk. The following sections therefore explain how this process of selecting services should work.

7.4.2 *Detection*

Since preventative measures in this strategy make sure that employees cannot use cloud services without pre-approval, detection cannot occur based on usage patterns, like in the previous two strategies. Instead, the only way in which services could be found to enter the whitelisting process is by either users from the business or the IT department suggesting an application they learned about externally.

7.4.3 *Analysis*

The analysis of cloud application in this scenario should not be based on it's detected usage pattern, since that is absent when the use of the application is blocked as expected in a whitelisting-scenario. Instead, the organization is likely to have a solution that has extensive knowledge of cloud services in order to be able to block these services in the first place. That solution could be a CASB (see section 6.6.1 It can then leverage the knowledge present in these solutions to do an initial analysis and weed out any services unlikely to get whitelisted. The remaining services can then be analyzed manually.

7.4.4 *Response*

After an application is analyzed, and the decision is made to whitelist that application, the organization needs to take the necessary technical measures to make that happen. In the simplest case, this may consist of a one time action removing any rules blocking that specific application. However, since many cloud services or platforms run on other platforms or infrastructure services themselves, they may frequently scale to domains or IP-addresses not in the current rule set (which would break whitelisted services) or scale down and abandon domains or addresses (which would allow unintentional whitelisting of services). Third party solutions, such as CASBs exist in order to mitigate this concern.

Once the application is correctly whitelisted, the organization could choose to provide added security features to the application, although the extent to which an organization is able to do that may be limited if the application is not provided by the IT organization, depending on the cloud application in question. First, organizations could provide users with the possibility to sign in using their corporate credentials, for example using an IAMaaS-solution (see section 6.6.2, allowing them to revoke access if necessary. Furthermore, they could leverage a CASB to enforce rules for encryption or restrict access to certain functionality, at specific locations or at different times.

7.4.5 *Evaluation*

Organizations following a whitelisting strategy should regularly evaluate through four main questions:

1. Whether their blocking of non-whitelisted applications works
2. Whether their process for selecting whitelisted applications works
3. Whether their efforts to provide their users with functionality (reducing the incentive to create CBSIT) is at balance with their efforts to suppress CBSIT when users do see incentive.
4. Especially if the answer to the previous question is 'no': whether this is because the strategy or measures do not fit the organization.

The first three of these evaluations are an evaluation of whether the measures they implemented are implemented correctly and are whether they work (doing things right), whereas the fourth question looks at whether there is a fit between the strategy and its related measures and the context of the organization.

7.5 PROHIBITING

In cases where the risks associated with CBSIT have an impact or likelihood sufficient enough to warrant mitigation, where no options exist for experimentation in a walled garden or controlled usage of Bring-your-own-App, one option that remains is focusing fully on suppression of all cloud services not directly under control of IT. Again, the aim is to have no Cloud-Based Shadow IT (CBSIT) at all, by removing all opportunity for unknown cloud services to be used, without exceptions. Since no exceptions are allowed, the prevention section is the only relevant step in this strategy. However, as the contents of that process step would be the same as in the "Whitelisting"-strategy, it is not repeated here.

7.6 CHAPTER SUMMARY

This chapter, at the start, set out to answer the third research question:

> What are possible strategies for managing Cloud-Based Shadow IT and how can they incorporate the measures from Question 2?

The answer consisted of a set of five strategies, where increasing degrees of influence where exerted over CBSIT that employees used.

Many organizations start out IGNORING Cloud-Based Shadow IT, perhaps employing a few ad-hoc initiatives that (unknowingly) influence its adoption in a positive or negative way.

For many organizations, the first step they take when recognizing that CBSIT is an issue MONITORING, creating visibility and employing some initiatives to increase the attractiveness of their central IT. The measures taken in this strategy remain relevant in the next three strategies as well, as creating insight into CBSIT-usage is a prerequisite for being able to influene it.

Organizations that choose to go further employ blocking mechanisms to enforce BLACKLISTING where certain services are blocked, WHITELISTING, where only selected services are allowed, or decide that PROHIBITING the use of all cloud-services not offered by their IT department is necessary.

Organizations choosing those last few strategies need a more comprehensive set of measures, balancing the fact that they try to block access to cloud services their employees think they need for their tasks with improvements in they way their IT department creates its own service portfolio, and by creating policies, management buy-in and awareness among employees in general to support their efforts in controlling CBSIT.

An important thing to note is that this is not a maturity scale: organizations moving further to the right (or left) in figure 7.1 are not necessarily improving

8

VALIDATION

In order to validate the findings and the design of the framework, four more interviews were conducted in addition to the informative interviews that were conducted in an earlier phase. This section chapter the findings from these interview. The four candidates had the following profiles:

- A Director of Sales Engineering for the EMEA region at a Cloud Access Security Broker vendor
- The CISO of a professional services firm
- The CISO of a Dutch municipality
- The interim CISO of a construction materials conglomerate

The first interview gave an insight into the view of a vendor of products specializing in the management of CBSIT. Such vendors see organizations varying in size, industry and geography, and can thus spot any omissions caused by the researcher's perspective.

The second interview provided further validation of the framework in isolation, from a CISO who has some experience in mitigating the risks from CBSIT and whose organization also advises clients on this subject.

In these interviews, the framework was explained, and participants were asked whether or not they agreed with the components, and why.

The third and fourth interview were different in nature, focusing more on how the framework matched what the CISO's of these organizations were doing, and how these efforts matched the recommendations from the framework.

The sections below give a summary of feedback where the interviewees either disagreed with, or specifically deepdived into, a part of the research. For the sake of brevity, other remarks have been added as references in relevant sections in the previous chapters.

The full interview transcripts can be requested from the author.

8.1 INTERVIEW 1 - CASB PROVIDER

The first expert interviewed for the validation of the framework was a sales engineer for a CASB-vendor, leading a team of technical engineers who worked with sales staff across a region comprising Europe, the Middle East and Africa. The vendor he works for is one of the larger players in the sector.

In general, he agreed with both the structuring of the framework in strategies and measures, and with the contents of both sections.

Going further, the expert argued that the risk of data security, in the sense of confidentiality, and the risk of damages resulting from non-compliance were overstated in most companies. He argued that the reliance on processes at these cloud vendors, with whom no SLA and exit-strategies are agreed in the case of CBSIT is in fact far greater for most organizations he had seen.

More specifically, he confirmed earlier findings that for many organizations, any risks of data breaches for data located at a CSP are surpassed by the risk of data leaks from their own systems if these organizations have limited capabilities to manage those in a secure way. A the same time he argues that moving to Shadow IT still does not solve all problems.

> Ik denk dat daar een waarschuwing of advies moet komen: voor organisaties waar intern een challenge is om hun IT veilig te managen, moet er niet uitgehaald worden naar Shadow IT, maar moeten ze met hun MSP of medewerkers kijken naar clouddiensten die dan in een officiëel account moeten worden gegoten. (...) als je als organisatie bijvoorbeeld je mail overzet naar persoonlijke Gmail-adressen, dan los je misschien op dat de Exchange-server vatbaar is voor traditionele hacks, maar je adresseert niet de compliance en data ownership en de toegang.

On the side of the advantages, he added improved collaboration opportunities as a specific example of improved productivity through CBSIT.

Although CASBs rely heavily on the ability to monitor network traffic, when discussing their various methods of interception he warned that the increasing speed of mobile networks (e.g. 3G and 4G networks) may impair that ability. He then added various technical measures that organizations can take to find a balance between making CBSIT adoption more difficult versus making the sanctioned way of working easier, or at least making a visible way of working easier through the use of IAMaaS-solutions.

8.2 INTERVIEW 2 - PROFESSIONAL SERVICES FIRM

The second expert interviewed for the validation was the Information Security Officer at an accountancy/advisory-organization, who had also provided input during the informative round of interviews [31].

One of the main points of focus, on which we had also touched during the informative interview, was the concept of Asset Based Services. While the traditional business model for this firm was to bill by the hour (although fixed-fee engagements occur as well), these services were based on renting out hardware or software. As these services were developed outside (control of) the IT-organization, they can be shared under the definition of shadow IT. Their nature as a commercial proposition make them distinct in the sense that responsibility for their creation and their ownership lies elsewhere else in the organization than for the functionality that Shadow IT in the stricter sense tries to fulfill. As a consequence, the definition section was updated.

A second discussion took place on the concept of blacklisting and whitelisting: could you have a combination of both? Could an organization have both a whitelist of approved and supported applications, a blacklist of applications it blocks access to, and a gray area in the middle? This was a subject that came back in the interview with the buidling materials conglomerate CISO, and in both cases it was concluded that although such a setup is possible; it is in essence a variant of a blacklisting strategy, taking the word "whitelist" from a different conceptual domain.

8.3 INTERVIEW 3 - MUNICIPALITY

The third interview took place with the CISO of a Dutch municipality. We first discussed the contents of the framework, and then its applicability for the municipal organization.

The municipality has about 150.000 inhabitants, and employs roughly 1400 FTE, supplemented with contractors.

The CISO split those 1400 FTE in two categories. The first category consists of employees executing predefined processes. For those employees, the municipality offers tooling that matches the requirements of the processes closely. As such the risk is limited as they are the group least likely to resort to CBSIT.

The other category are knowledge workers, who generally work in projects where the demand for tooling is often hard to predict. When discussing the risks of CBSIT, the CISO focused primarily on this group.

The primary risk category that the CISO saw as applicable to this category was the loss of continuity as data and applications, that knowledge workers brought in using their personal credentials to support their tasks, became unavailable. At the same time, people leaving the organization would still have access to this data. The leaking of that data is a concern.

He was less concerned about other risks, such as data breaches as cloud providers were hacked or the risk of non-compliance.

At the time of the interview, the municipality's viewpoint best matched the Monitoring strategy. They periodically review both network logs and financial statements in order to find shadow services that were used by individuals and departments. For departments, the response is often to counter inefficient procurement and out-of-budget spending by offering that the IT department takes over the management of the service. Many departments agree as they do not actually want to manage an IT service, but have come to do so by chance. Regardless of their response to the proposal, as the CISO argued, these services seldom carry very much risk. If they do, the CISO argued that these services' owners are often persuaded to take mitigating measures when this risk is translated from a technical risk into a risk that is applicable to the service owner's business perspective, i.e. by translating the risk of loss of data to a risk of continuity for the business process that relies on it and for which the service owner is responsible.

For individual instances, the situation is more complex. Although the CISO admitted not having an exact insight into how much CBSIT individual users have adopted, he said. It may be possible to discuss their shadow cloud consumption with individual employees, but in reality and with finite resources it is not a feasible option to to so with all but the largest users. There is currently no real time connection monitoring solution, which makes automating the process difficult.

At the same time the visibility of shadow cloud usage for these employees is dropping. They bring more and more private devices into the workplace that are not always connected to the municipality's monitored network, and the CISO expected that number to grow. This makes it more and more difficult to take measures that guarantee that the municipality is able to monitor and block their employees' cloud usage.

The CISO's proposed response was threefold. The first part was to make sure that the dialogue with users would stay open. Since it would be difficult to guarantee detection in a technical measure, closing down a verbal communication channel to users by being overly restrictive would be the last thing to do.

The second measure is to actively respond to the demand of users by introducing functionality that replaces the largest volumes of SIT. Again: it would be difficult to prevent users from accessing shadow services, but by making it easy to use the sanctioned alternative, the CISO hoped to reduce the amount of CBSIT.

The third measure was to regain some control over what employees used, by creating a presence on their devices. In return for allowing them to use sanctioned services and the data they contain on their device (and thus sparing them the hassle of extracting data from the municipality's infrastructure), the municipality would require a mobile device management solution that would take care of containerization of the applications and enforcement of security policies. This control over devices, combined with a to-be-introduced solution for filtering and blocking connections would move them towards a situation where they would be able to block some services that they considered to pose an excessive risk.

These measures, especially the last one, show how much the topic of CBSIT is interwoven with other developments in an organization's context. Although the framework, as the CISO rightly mentioned, features a rather technocratic and isolated approach to the problem of CBSIT (which is, to an extent, required to focus on a clearly defined scope), organizations have to consider various factors outside of this scope in order to come up with a wholesome approach.

8.4 INTERVIEW 4 - CONSTRUCTION CONGLOMERATE

The fourth interview took place with an Information Security Officer of a construction conglomerate. We discussed both the contents of the framework, and its application to the organization.

That organization, as a holding company of a group of independent entities, employed about 80,000 people, and generated €24 billion in annual revenues. The organization is publicly traded at various exchanges, including an American one, and is therefore required to comply to the Sarbanes-Oxley act[1].

It is heavily diversified, with over 1000 operating companies. These operating companies ranged from factories to retail outlets and building companies. Many were acquired in a variety of deals, and were allowed to remain largely independent in terms of their information systems. At the time of the interview, the company was just going through a large round of acquisitions following the merger of two other players who had to divest some of their entities to maintain competition in national markets.

In most of these acquisitions, it is necessary to "carve out" the company from its parent, and make sure that it is up and running independently as soon as possible. Integration with the new parent company is given lower priority. As a result, the group had a myriad of networks, Active Directories, local IT departments and databases outlining their IT infrastructure (CMDBs).

There were some central IT functions, which provided services to entities that chose not to create their own implementations, but there were no mandatory services at the time of the interview. When discussing the applicability of the framework, it became apparent that the framework's focus on organizations with a somewhat centralized IT function did not fit with this organization. In some ways, services not known by the central IT department could be classified and treated as SIT, thus allowing discussion about the framework, but always with the caveat that this decentralized nature is by choice, and not an unwanted phenomenon.

It seemed likely that the organization faced some of the risks outlined in chapter 5. In particular, group recognized the risk of inefficient procurement throughout all of the entities. Risks such as data security and continuity were thought to be handled at the entity level, with entities working with more sensitive data or more IT-dependent processes paying more attention to these factors in their own sourcing choices. There was some attentiont to compliance, in particular compliance with SOx, for which services impacting financial reporting in a material way at the larger entities were required to report on their controls.

Following both the limited set of risks that were considered relevant at group level, and the limited priority that was given to security in general and to mitigating these risks specifically, the group (unknowingly) followed the ignoring strategy.

> We zijn nu onbewust onbekwaam en gaan langzaam naar bewust onbekwaam, en zo zetten we stappen.

At the same time, the organization did work on the risk they recognized the most: the inefficiency of procurement of similar services throughout various entities. A project had been started transfer every instance of collaboration

software in European entities to a single contract for a collaboration service from a CSP, thereby cutting costs. This approach of offering centrally procured functionality that better aligned with apparent demand was aimed primary at mitigating the problem of high cost at each individual entity.

The Information Security Officer recognized that a step towards a monitoring strategy would be valuable in order to gain insight in what services were used and better assess risk and evaluate further measures and strategies, but at the same time argued that the step towards implementing monitoring for such a large and diverse set of separate entities and individual locations did not fit the overall maturity level of the group when it came to IT.

8.5 SUMMARY AND DISCUSSION

This chapter contains the findings from interviews conducted to validate the findings of this thesis. This section draws a conclusion from these findings.

In general, it is safe to say that the experts agreed with both the structure of the research and with the contents of the various components. Although they often had remarks adding nuance to some of the findings or placing them in the perspective that their line of work gave them, there were none that disagreed with the choices I made and the remarks have been integrated into the previous chapters.

The last two interviews were the most insightful, as their goal of testing the framework not only to the agreement of experts on a conceptual level, but rater revealed the limitations of the framework proposed in this thesis when directly applied in actual organizations.

In the fourth interview, it became apparent that the black-and-white approach to whether something is "Shadow IT" or "Central IT", as Storey et al. [59] pose it, is far more difficult to answer in organizations with a heavily decentralized nature. In addition, it is much more difficult to take any measures once you have made the decision that certain types of systems are "Shadow IT", since the myriad of technologies and maturity levels requires tailoring at the levels of individual entities.

This could be solved by applying the framework in multiple instances at these lower, more decentralized, levels, requiring the entities to provide assurance about their control over CBSIT towards the group entity. Each entity may choose its own strategy and its own measures in order to reach the level of assurance that the group's security and compliance departments require. Some may decide to monitor, reporting their findings and their evaluations regularly towards the group CISO. Others may work with blacklists or whitelists and report on the contents of those lists, as well as the evaluation of their effectiveness to create a centralized dashboard for a group CISO.

At the same time, this interview put the whole concept of CBSIT into perspective in an organization that had a very low maturity for their IT in general, and IT security in particular. Although earlier chapters stated that organi-

zations should use the section on risks and opportunities to assign a level of priority to their aspirations in managing CBSIT, the explanation of this organization's challenges made it clear how it came to be that many organizations have not addressed it at all.

The third interview was particularly insightful as it showed how even a more mature organization that had recognized and somewhat prioritized the management of CBSIT found it challenging to translate the measures from their abstract description in literature to a workable situation in practice. It was useful to gain the insight that the approach was, as the interviewee stated it, technocratic. I do no see this approach as a fault, as it is somewhat of a requirement when studying a phenomenon to limit the scope of the study. However, it is good to note that in order to really control CBSIT, anyone who uses the framework should consider as a starting point, and add specific knowledge of their organization.

The third interview was also the interview where it was most explicitly stated that the CISO considered the fact that personal accounts were used for CBSIT, and the various risks originating from that, the biggest problems. Other experts shared the opinion that this is problematic, but made it less explicit.

9 CONCLUSION

This chapter contains the conclusions of the research described in this thesis. The thesis started with a problem statement; the lack of a framework to control Cloud-Based Shadow IT.

The main research question rephrased the problem statement:

> What is a framework that helps organizations control Cloud-Based Shadow IT?

This research then posed three knowledge questions in order to gain the knowledge required to form a framework:

1. What are causes and effects associated with Cloud-Based Shadow IT? (Section 9.1)
2. What are measures for managing Cloud-Based Shadow IT? (Section 9.2)
3. What are possible strategies for managing Cloud-Based Shadow IT and how can they incorporate the measures from Question 2? (Section 9.3)

The sections below briefly summarize the answers to these knowledge questions, and uses them to answer the main research question.

9.1 CAUSES AND EFFECTS

The first sub-question is:

> What are causes and effects associated with Cloud-Based Shadow IT?

to answer the research question, this thesis first looked at causes and affects f CBSIT. A combination of a literature review and expert interviews revealed the primary drivers of CBSIT to boil down to a few main points.

These points were a combination of causes from traditional shadow IT, which were found to be well described in literature, the properties of cloud services (e.g. ease of deployment) and the trend of consumerization. In brief: users choose to deploy services similar to those they use at home, because it is easier than using the sanctioned alternative or requesting better tooling from IT. Figure 9.1 shows an overview of the causes and effects that were found.

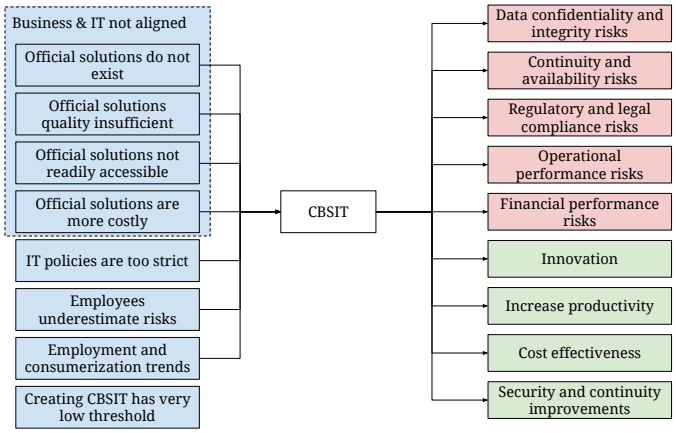

Figure 9.1: An overview of the categories of causes and effects found as an answer to Knowledge Question 1

9.2 MEASURES

The second sub-question is:

> What are measures for managing Cloud-Based Shadow IT?

As an answer to this sub-question, chapter 6 introduced a process consisting of five steps to structure the applicable measures. Figure 9.2 shows these measures.

As scientific literature focused primarily on the management of traditional SIT, the interviews were a valuable source of information as input for this section. On the topics where both the literature and experts provided input, these inputs aligned quite well.

Looking at the final list of measures, it can be concluded that these measures relate back to the causes and effects as displayed in figure 9.1, as they either impact the causes of CBSIT by removing incentives, raising the bar for adopting CBSIT or by responding to the effects by mitigating the risks that CBSIT poses once it is adopted. Table 6.3 in chapter 6 shows this.

Prevention	Detection	Analysis	Response	Evaluation
Create policy on (shadow) cloud usage	Stimulate dialogue with business users	Create automatic CBSIT risk rating	Take corrective action based on policy	Evaluate if strategy is still appropriate
Create awareness of CBSIT-risks	Monitor financial statements	Create manual CBSIT risk rating	Provide extra awareness training	Evaluate if measures are still appropriate
Implement filtering or blocking technology	Monitor connections		Update blacklist / whitelist for filtering	Evaluate strategy and measure effectiveness
Increase IT awareness of business demands			Provide extra security for shadow service	
Reduce time to contract			Transfer control of service to IT	
Reduce time to provisioning				

Figure 9.2: The measures discussed in chapter 6

9.3 STRATEGIES

The third sub-question is:

> What are possible strategies for managing Cloud-Based Shadow IT and how do they use the measures from Question 2?

As an answer to this sub-question, chapter 7 introduced five strategies for an organization's approach towards CBSIT. They are shown in figure 9.3

By defining the strategies and the measures that are relevant for these strategies, the framework takes shape, as can be seen in figure 9.4.

As said before, the literature on SIT predominantly describes the traditional form, and rarely provided strategic advice as it often did not consider SIT a recurring and widespread phenomenon that warranted a conscious choice that would set the baseline for future occurrences of CBSIT: many articles described ad-hoc treatment of shadow systems.

As such, the strategies in this thesis were formed in discussions with various people during the research, and are based on general principles of decision making in other contexts where some form of filtering is relevant.

9.4 ANSWERING THE MAIN RESEARCH QUESTION

This report has worked towards answering the main research question and solving the problem that there is no framework for managing CBSIT. Figure 9.4 shows an overview of the framework, as a path for organizations that want to gain control over CBSIT. This thesis has shown that management of CBSIT is, first and foremost, based on risk management. It is essential that organizations understand the risks they face, or do not face, before taking action.

It has then shown that a framework for managing CBSIT is composed of various measures, which are more or less difficult to implement for each organization. These measures have impact on either the causal side of CBSIT, or on the effects: they prevent its creation, or mitigate its effects. Organizations should take input from their risk analysis and from actual data in order

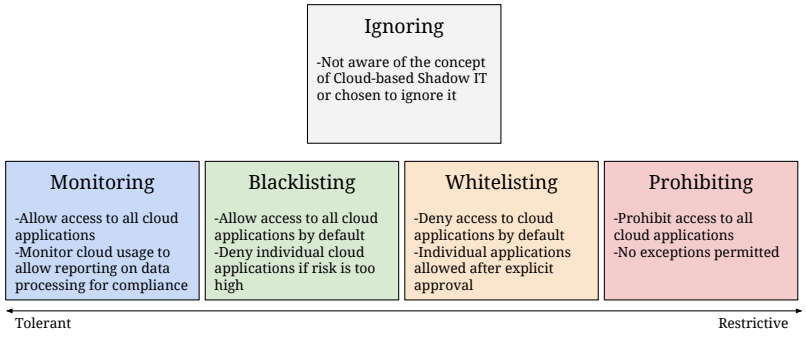

Figure 9.3: The five strategies explained in chapter 7

to determine whether certain measures are appropriate, and fitting for their maturity level.

Finally, it has shown that in order to implement these measures in a coherent way, it is necessary that an organization chooses one overall strategy, which guides both the final choice of which measures are needed, but also how they are applied. These strategies vary in impact and required effort, and choice should again be based on the risk analysis, as well as the risk appetite of the organization.

By building on this framework, expert interviews have shown that organizations believe that the challenge of managing CBSIT is not an impossible one.

9.5 VALIDATION

The validation, through interviews with four experts, lead to the conclusion that the framework in itself is sound. Experts by and large agreed with both the setup: to identify risks, choose a strategy and then select appropriate measures, and with the contents of these steps.

Criticism primarily focused on two things. One: its applicability in decentralized organizations consisting of highly autonomous entities with low maturity in terms of IT(-security).

Two: its 'technocratic', or rather isolated approach to a phenomenon that is very interconnected with various other challenges that organizations face.

Both of these point are valid concerns, and require that every organization uses the framework as a starting point from where a further analysis is based on the organization's unique characteristics.

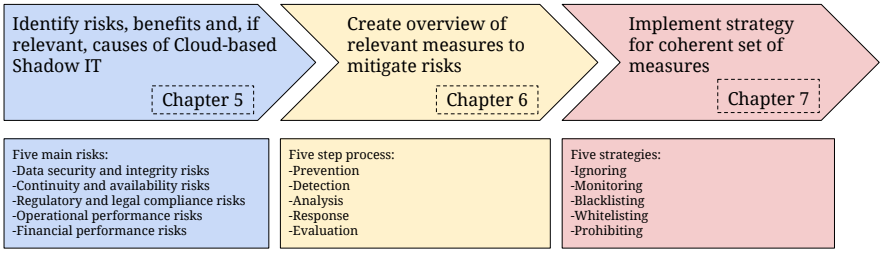

Figure 9.4: Overview of the framework

10 DISCUSSION

Validation interviews have shown the value of this research, contributing to the understanding and management of Shadow IT in the cloud era. Some limitations apply, and there is plenty of room for further research in this area.

10.1 CONTRIBUTIONS TO SCIENCE

The first input to answer the knowledge questions was a review of existing literature. After this review, which is described in section 3.3, the questions were not yet answered, but further work was performed. This thesis thus contributes this further work to the scientific field on the following key points: First, it has gathered all of the available literature on SIT, and collected from those the causes, effects and measures that were applicable to CBSIT. It added specific literature on CBSIT, where that was available, thus providing a clear overview for future practitioners seeking to build on existing literature.

Second, it enriched what was found in literature. This happened both by interviewing experts and by finding additional sources that provided information on the causes, effects and measures that were identified earlier. These sources could be scientific literature from another perspective or field, or by incorporating sources outside scientific publishing as developments in this field often take place outside academia.

Third, it added a structure. Existing literature, when it mentioned causes, effects and measures, often did this in unstructured lists, casual mentions in text and in diagrams. This thesis has added structure in the form of a five step process to align taking these measures with other works on organizational processes.

Fourth, it added strategies as an overarching approach. For these strategies, a first start was made at describing how the various measures should be implemented to control causes and effects.

These contributions were then validated through expert interviews.

Further research should build on these contributions. The last section of this chapter includes proposals for how.

10.2 CONTRIBUTIONS TO PRACTICE

The literature review mentioned earlier did not only include scientific material. Professional material was included as well. it was in many ways similar to the academic material. Two observations stood out.

First, frameworks for control of IT often lacked either attention for cloud computing or for aclSIT. Several control frameworks were considered in choosing the five process steps in chapter refch:measures and in finding the measures themselves, and none paid attention to both.

Second: many lists containing recommendations were very ad-hoc, listing measures that one could take, but without a wholesome approach.

The contribution to practice, thus, is again the fact that a comprehensive set of causes, effects, measures and strategies was presented in a structured form, meaning that organizations can now use the model in figure 9.4 as a start of their efforts to control CBSIT or, taking a step back, creating awareness of CBSIT in various levels of the organization.

Although some further work may be needed (see below), and the framework requires tailoring to each organization, this is a first step towards controlling a phenomenon that many organizations don't yet know about.

10.3 LIMITATIONS AND FUTURE WORK

A first idea for future work was given during the third validation interview, and concerns quantification of the phenomenon and resulting risk. The problem statement of this thesis cites several sources that consider CBSIT a problem worth discussing, however, but there is limited data on how large the problem is. CASB-vendors regularly publish statistics on shadow cloud usage [56]. There is a caveat in using these statistics: it is in these vendors' interest to report relatively high numbers, and these numbers might vary wildly by geography, industry and organizational size.

Furthermore, the published number is often the number of cloud services that are used. During the first round of interviews, several of the experts argued that a better construct to indicate the risk that organizations are exposed to through the use of CBSIT would be useful. Input for such a construct would not only be the number of services, the properties of each service and the amount of data (as many CASBs can provide), but also the nature of this data, provided that the organization has DLP and data classification measures in place. Ideally, a risk rating for an organization or the reliance of processes on the CBSIT. Better research outlining the above in terms of likelihood and potential impact would help organizations better assess the need for moving out of the "Ignoring"-strategy.

Another limitation, and starting point for future research, is the notion that this thesis is written with the assumption of a somewhat centralized form of IT and IT risk control. Although it is still applicable if IT control is distributed throughout the organization, it is currently up to the reader to estimate the effects of various governance models on the framework. Further research could dive into these effects, and provide additional input for the answers to the research questions federated or laissez-faire approaches.

The separation between different forms of technology that users maintain, as

discussed in the second validation interview [32], would be another governance-related subject for further research. In addition to SIT as covered in this research, user-developed artifacts may include technology which Berray and Sampath [5] place under the CTO, and which are directly monetized. This thesis has excluded that technology from its scope, but it may well be worth looking into.

The points above mainly concern limitations caused by the scope of the research in terms of breadth. Some limitations in terms of depth apply as well.

For example, the measures that were found were only validated through interviews, whereas a more extensive research, of a different nature, could seek to apply them in practice and study their effects.

How does blocking one service lead to circumvention by using different ones? What would be good ways of creating better security awareness about CBSIT? How well do various structures of CASB-implementations work, given limitations on controlling cloud usage when the network, device and applications are outside of the organization's control? How well does providing single-sign-on-capabilities to users through an IAMaaS-solution mitigate the risks resulting from personal accounts with cloud services?

Such knowledge would also serve to solve another limitation of the framework, which is the somewhat abstract and high level nature. The framework is not yet a guide for controlling CBSIT. Since CBSIT is a name for a wide variety of services, used in a wide variety of different organizations, the answers to all of the research questions are necessarily broad, so as to cover the many possible scenarios, and lack detail, because describing all possible scenarios would yield an unwieldy document. More in-depth and practical research could solve this by providing detail for scenarios that were determined to be common.

10.4 PERSONAL REFLECTION ON THE PROJECT

After having discussed and reflected upon the contents of this thesis and its implications for the future, this section looks back on the project of writing the thesis.

The first point that comes to mind when looking back is how difficult it is to imagine the end product when starting a project like this. Although the project started with the idea to write something interesting on CBSIT, which proved an interesting and upcoming subject even after a few minutes of searching, it took quite a while for the idea for the exact result (the framework) to take shape. The fact that a framework is quite a loosely defined term didn't help with this. I now recognize the value that a subject like "Research Topics" could have: forcing you to have a proposal that is much more detailed in what it wants to achieve, as more literature research is already done. This also forces a clear separation between what is found in literature and what is found elsewhere.

Flowing from the fact that the final product was not precisely defined for a long time, I have postponed several activities, expecting that time (and more writing) would bring clarity. The most important of these activities were both rounds of interviews, where hesitation to appear at an interview unprepared (as well as agendas) caused me to schedule them relatively late in my research in both cases. At the time of the interviews, that fear turned out to be unnecessary and the interviews were, in many ways, the most interesting parts of the project. They were both a good source of information, and a good way to test the demand for the intended result.

This illustrates an interesting factoid that I encountered a while back: becoming more skilled leads to better insight in what you don't know, causing a lack of confidence (simplified). It is an instance of the Dunning-Kruger-effect (see Kruger and Dunning [41]). In a future project, this would be the main pitfall to prevent, and would lead to both timelier and more complete results.

In the end, it comes down to motivation. Staying motivated to work on a project this long is difficult for me, regardless of how interesting I think the subject is. Approaching deadlines, for me, add to motivation, so setting more ambitious deadlines would be an improvement.

Overall, I am quite happy with how both the project and the result turned out. Dear reader: thanks for reaching the end.

BIBLIOGRAPHY

[1] 108th Congress of the United States of America. Sarbanes-Oxley Act of 2002, 2002. URL 1.usa.gov/1SyK7Og.

[2] S. Behrens. Shadow systems : the Good , the Bad and the ugly. *Communications of the ACM*, 2009.

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

[4] C. A. Bellino, D. Ochab, and J. S. Rowland. (GTAG14) Auditing User-developed Applications. Technical report, The Institute of Internal Auditors, 2010.

[5] T. Berray and R. Sampath. The Role of the CTO: Four Models for Success. *Aorn*, 75(1):102–112, 2002. ISSN 00012092. doi: 10.1016/S0001-2092(06)61717-1.

[6] Booz Allen Hamilton. Shining the Light on Shadow Staff. 2004.

[7] O. Bossert, C. Ip, and J. Laartz. A two-speed IT architecture for the digital enterprise. *McKinsey*, pages 1–6, 2014. URL http://bit.ly/1wIg8aE.

[8] O. Bossert, J. Laartz, and T. J. Ramsoy. Running your company at two speeds. *McKinsey Quarterly*, pages 1–3, 2014.

[9] B. Bulgurcu, H. Cavusoglu, and I. Benbasat. Information security policy compliance: An empirical study of rationality based beliefs and information security awareness. *MIS Quarterly*, 34(3):523–548, 2010. URL http://bit.ly/1OgqnqE.

[10] Center for Internet Security. The Critical Security Controls for Effective Cyber Defense. Technical report, 2014.

[11] W. Chan, E. Leung, and H. Pili. Enterprise risk management for cloud computing. Technical report, COSO, 2012.

[12] P. Cichonski, T. Millar, T. Grance, and K. Scarfone. Computer Security Incident Handling Guide. Technical report, National Institute for Standards and Time, 2012.

[13] CISO of a Dutch municipality. Validation Interview, 2016.

[14] R. H. Coase. The nature of the firm. *Economica*, 4(16):386–405, 1937. ISSN 00130427. doi: 10.2307/2626876.

[15] C. Coles, J. Yeoh, and H. Braon. The Cloud Balancing Act for IT : Between Promise and Peril Table of Contents. Technical report, Cloud Security Alliance.

[16] P. D'Arcy. CIO strategies for consumerization: The future of enterprise mobile computing. *Dell CIO Insight Series*, pages 1–15, 2011. URL http://dell.to/1QpOTXT.

[17] B. Darrow. Guess what Mr. CIO? One in five of your employees uses Dropbox at work, 2012. URL http://bit.ly/23w7dIO.

[18] Director of Sales Engineering at a CASB Vendor. Validation Interview, 2016.

[19] W. J. Elemans. Shadow IT: how to respond to the chaos emerging from the shadows ? 2014.

[20] European Parliament and Commission. Directive 95/46/EC of the European Parliament and of the Council, 1995. URL http://bit.ly/1Qm5RpW.

[21] Former Chief Information Security Officer for a large Dutch Bank. Informative interview, 2015.

[22] Former Chief Information Security Officer for an intergovernmental organization. Informative Interview, 2015.

[23] D. Fuerstenau and H. Rothe. Shadow IT Systems: Discerning the Good and the Evil. *ECIS 2014 Proceedings*, pages 0–14, 2014.

[24] Gartner. Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond, 2012. URL https://www.gartner.com/newsroom/id/1862714.

[25] A. Gyoery, A. Cleven, F. Uebernickel, and W. Brenner. Exploring the shadows: IT governance approaches to user-driven innovation. *Proceedings of the 20th European Conference On Information Systems (ECIS)*, pages 1–13, 2012. URL http://www.a2research.com/.

[26] S. Haag. Appearance of Dark Clouds? - An Empirical Analysis of Users' Shadow Sourcing of Cloud Services. pages 1438–1452, 2015.

[27] T. Hardjono, N. Klingenstein, and S. Cantor. SAML Version 2.0 Errata 05. (May):1–44, 2012. URL http://bit.ly/1TqUUde.

[28] N. Heath. How to manage shadow IT without driving it underground, 2014. URL http://tek.io/24aoFTC.

[29] R. Holdgrafer. Managing Shadow IT, 2015. URL http://bit.ly/1R8m71g.

[30] Information Security Officer of a construction materials conglomerate. Validation Interview, 2016.

[31] Information Security Officer of a professional services Firm. Informative Interview, 2015.

[32] Information Security Officer of a professional services firm. Validation Interview, 2016.

[33] International Organization for Standardization. ISO 27035:2011. Technical report, International Organization for Standardization, 2011. URL http://bit.ly/1XxVt4e.

[34] ISACA. Incident Management and Response. Technical Report March, 2012. URL http://bit.ly/218S6mA.

[35] J. Kalter. Think Like an Attacker. Technical report, Core Security, 2014.

[36] R. N. Katz. *The Tower and The Cloud*, volume 28. 2008. ISBN 9780967285399. doi: 10.1161/ATVBAHA.107.151787. URL http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+Tower+and+The+Cloud#0.

[37] G. Killcrece. Incident Management. Technical report, US Department of Homeland Security, 2005. URL http://1.usa.gov/1Kq7s22.

[38] J. King. The upside of Shadow-IT, 2012. URL http://bit.ly/1TqV58u.

[39] S. Koeffer, K. Ortbach, I. Junglas, B. Niehaves, and J. Harris. Innovation Through BYOD? *Business & Information Systems Engineering*, pages 1–13, 2015. ISSN 2363-7005. doi: 10.1007/s12599-015-0387-z. URL http://dx.doi.org/10.1007/s12599-015-0387-z.

[40] Koningrijk der Nederlanden / Staten-Generaal. Meldplicht Datalekken, 2015.

[41] J. Kruger and D. Dunning. Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of personality and social psychology*, 77(6):1121, 1999.

[42] J. Kuhn. Expanding the Expanded Incident Lifecycle, 2009. URL http://bit.ly/1LtL2I9.

[43] S. Ky. Managing Consumerization of Personal Cloud Storage: A New Zealand Perspective. (June):97, 2014. URL http://bit.ly/1XxVEwD.

[44] D. Linthicum. Shadow IT comes out of the shadows - and back into IT. URL http://bit.ly/1Kq7BCL.

[45] A. Mann, G. Watt, and P. Matthews. *The Innovative CIO*. Apress, Berkeley, CA, 2013. ISBN 978-1-4302-4410-3. doi: 10.1007/978-1-4302-4411-0. URL http://bit.ly/1TnK4Ud.

[46] NIST. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. Technical report, 2011. URL http://bit.ly/1Qm6znm.

[47] C. Null. 5 things IT Ops can do about shadow IT on the cloud, 2015. URL http://techbeacon.com/5-things-it-ops-can-do-about-shadow-it-cloud.

[48] OAuth Working Group. OAuth Community Site. URL http://oauth.net/.

[49] OpenDNS. Ensure Shadow IT Security with the Cloud Services Report, 2015. URL http://bit.ly/1OgqVwJ.

[50] Palo Alto Networks. Decryption - PAN-OS Administrator's guide. Technical report, 2015.

[51] Product specialist at the Ministry of Defense. Informative Interview, 2015.

[52] PWC. The five behaviors that accelerate value from digital investments: 6th Annual Digital IQ Survey. Technical Report March, PWC Digital IQ, 2014. URL http://www.pwc.com/us/en/advisory/digital-iq-survey/assets/6th-annual-digital-iq.pdf.

[53] N. Raden. Shedding light on shadow IT: Is Excel running your business? *Hired Brains Inc., Santa Barbara*, (January):11, 2005. URL http://bit.ly/20ZqOT9.

[54] C. Shapiro and H. R. Varian. *Information rules*, volume 32. Harvard Business Press, 1999. ISBN 087584863X. doi: 10.1145/776985.776997.

[55] P. Shaw. Intervening in the shadow systems of organizations: Consulting from a complexity perspective. *Journal of Organizational Change Management*, 10(3):235–250, 1997. ISSN 0953-4814. doi: 10.1108/09534819710171095.

[56] Skyhigh Networks. Cloud Adoption and Risk in Government. Technical report, Sky High Networks, 2015.

[57] K. Smyth and J. Freeman. Blue prism rogue IT survey 2007. Technical report, 2007. URL http://bit.ly/1QleaZs.

[58] R. M. Steinberg, M. E. Everson, F. J. Martens, and L. E. Nottingham. Enterprise Risk Management - Integrated Framework. *Coso*, 3(September):1–16, 2004. ISSN 14775360. doi: 10.1504/IJISM.2007.013372. URL http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf.

[59] V. C. Storey, L. Chen, and C. E. Chua. Central IT or Shadow IT ? Factors Shaping Users' Decision To Go Rogue With IT. pages 1–14, 2014.

[60] Stratecast | Frost & Sullivan. The Hidden Truth Behind Shadow IT Six trends impacting your security posture. Technical Report November, 2013. URL http://intel.ly/1PQWb7R.

[61] D. Strong, O. Volkoff, and M. Elmes. ERP Systems, Task Structure, and Workarounds in Organizations. *AMCIS 2001 Proceedings*, page 204, 2001.

[62] Symantec. Avoiding the Hidden Costs of the Cloud. pages 1–23, 2013. doi: 10.1002/fut.

[63] S. Thatte and N. Grainger. Feral Systems: Why Users Write Them and How They Add Value. In *Fifth Pre-ICIS workshop on ES Research*, number October, St. Louis, 2015.

[64] The OpenID Foundation. OpenID Foundation Website. URL https://openid.net/.

[65] R. Walters. Bringing IT out of the shadows. *Network Security*, 2013(4):5–11, apr 2013. ISSN 13534858. doi: 10.1016/S1353-4858(13)70049-7. URL http://linkinghub.elsevier.com/retrieve/pii/S1353485813700497.

[66] R. Werlinger and D. Botta. Detecting, analyzing and responding to security incidents: a qualitative analysis. *Proceedings of the EECE 512 Mini-conference on Computer Security*, pages 24–34, 2007. doi: 10.1145/1280680.1280702. URL http://dl.acm.org/citation.cfm?id=1280702.

[67] J. Wetherill. Going Rogue with PaaS: Bringing Shadow IT into the Light, 2015. URL https://www.activestate.com/blog/2015/01/going-rogue-paas-bringing-shadow-it-light.

[68] R. J. Wieringa. *Design science methodology for information systems and software engineering*. Springer, 2014.

[69] J. F. Wolfswinkel, E. Furtmueller, and C. P. M. Wilderom. Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, (September): 1–11, nov 2011. ISSN 0960-085X. doi: 10.1057/ejis.2011.51. URL http://www.palgrave-journals.com/doifinder/10.1057/ejis.2011.51.

[70] L. Zejnilovic and P. Oliveira. Employees as contributors of self-developed solutions. In *DRUID Academy 2013*, pages 0–27, 2013.

[71] S. Zimmermann and C. Rentrop. On The Emergence of Shadow IT - a Transaction Cost-Based Approach. *European Conference on Information Systems*, pages 1–17, 2014.

[72] S. Zimmermann, C. Rentrop, and C. Felden. Managing Shadow IT Instances: A Method to Control Autonomous IT Solutions in the Business Departments. *Americas Conference on Information Systems*, pages 1–12, 2014.