Linköping University | Department of Management and Engineering
Master's thesis, 30 credits| Master's programme in IT & Management
Spring 2023| LIU-IEI-FIL-A--23/04327--SE

Understanding the Impact of Cloud-Based Shadow IT on Employee and IT-Manager Perceptions in the Swedish Tech Industry

Adam Fager

Supervisor: Gianluigi Viscusi
Examiner: Viktor Arvidsson

Linköping University
SE-581 83 Linköping, Sweden
+46 013 28 10 00, www.liu.se

Preface

I wish to dedicate a thank you to my supervisor for this master essay, Gianluigi Viscusi. A university lecturer and PhD in Information Systems at Linköping University, who have assisted and given valuable advice during the writing process. I also wish to show my gratitude to the participants in the study for taking the time to answer the survey and be a part of the interviews.

- *Adam Fager, May 2023*

Abstract

This study focuses on the impact of Cloud-Based Shadow IT on data privacy in the tech sector of Sweden. It explores the use of unapproved applications by employees without the knowledge and control of the IT department. The objective is to understand how Cloud-Based Shadow IT affects employees' compliance with cloud services and to examine the understanding of IT managers regarding this phenomenon. The research problem addresses the challenges faced in ensuring compliance with regulations and effective utilization of cloud technology. By identifying the strengths, weaknesses, possibilities, and risks associated with Cloud-Based Shadow IT, this study aimed to provide insights for companies and IT managers in making informed decisions. It explores the relationship between Shadow IT and cloud services and investigates employees' and IT managers' adherence to and understanding of these issues.

The findings indicate that employees have varying levels of understanding, with limited knowledge of approved cloud services. Managers prioritize security concerns, including data compliance and ownership, but lack strategies to address knowledge gaps. The use of Cloud-Based Shadow IT has both positive and negative consequences, including increased productivity and collaboration but also data loss and non-compliance risks. Factors such as education and awareness of security risks are important for employees to understand and comply with policies. Overall, the study highlights the need for continuous education and awareness programs to improve understanding and decision-making regarding cloud services and Shadow IT.

Key words: Cloud-Based Shadow IT, Shadow IT, Swedish Tech Sector, Data Privacy, Managers, Employees, End User Computation, Workaround, Personal IT, Third-Party Access

1. Introduction

Cloud services: The vast new landscape that has helped businesses become more efficient. Employees become more flexible and have made productivity skyrocket through the roof. Where possibilities are endless and new rewards for companies that were imaginable before. At a first glance at least, cloud services are brilliant, effective, and easy to learn. Managers are eager to implement them, and employees seem eager to adopt them. Is this all the truth? To some degree, it is. The benefits of cloud services are undeniable. It gives organisations increased flexibility and scalability of their resources while at the same time being cost-friendly (Wafa'a & Khalid, 2020). Employees also view cloud services highly, as they provide extra help in performing more effective work and finding new solutions for work tasks. However, as cloud services become more prevalent in society, difficulties arise, particularly in ensuring that the appropriate cloud services are in use and are being handled by the IT department (Rentrop & Zimmermann, 2012).

Furthermore, it is important that the cloud services used in organisations are used by employees in a way that preserves the security of customers' data. The usage of cloud services is regulated by government rules that corporations must abide by, making data compliance and regulation crucial components for IT departments. In turn not following up on the usage of these services can lead to non-compliance, which increases the risk of hefty penalties, legal action, and reputational harm (Walters, 2013). Despite these policies in place, there are parts of cloud services used in organizations that management can have a hard time analysing to determine if they adhere to the policies (Walterbusch et al., 2017)

One area of concern for management is Shadow IT, which refers to the use of information technology solutions that do not have approval from management. It can manifest in the form of software, hardware, and information systems used by different departments or individuals in an organisation (Rentrop & Zimmermann, 2012). While Shadow IT is a known and studied phenomenon, research on the usage of Cloud-Based Shadow IT among employees is limited (ReRez Research, 2012). The increased rate of cloud services makes importance to dive in and study how IT managers are

knowledgeable about the use of cloud-related services by their employees. Moreover, it is important in their use as an extension of existing IT department solutions. This thesis aims to explore the impact of Cloud-Based Shadow IT on businesses in the tech sector, focusing on data privacy and compliance. It will investigate how well employees understand company policies regarding Cloud-Based Shadow IT and how IT managers handle and understand the complexities associated with it.

1.1 Background

The technology industry is constantly changing, and the advent of cloud services has completely changed how data is handled, used, and stored. Business organizations of all sizes can now access information and services on demand and with significant financial savings because of this type of data management methodology. Sweden is one country where the adoption of cloud services is progressing rapidly. During the years of 2016 to 2018 Sweden saw an increase in cloud service usage from 32% to 42% in enterprises (SCB, 2018). In 2021 it ranked as the top country in Europe in terms of cloud service adoption, with 75% of companies in Sweden having some form of cloud-based solution (Eurostat, 2021). However, despite the many benefits of cloud services and their increased popularity, businesses and organisations now face new difficulties.

The emergence of cloud services has introduced new standards to ensure that corporations comply with privacy laws, data protection, providing instructions to retain and utilize them. Unfortunately, not all firms and employees are aware of the industry rules and policies established by their organizations. This lack of awareness leaves them unfamiliar with recommended practices when working with cloud services. As the use of cloud services continues to grow, employees are turning to alternative methods to complement existing IT solutions. Shadow IT is an approach that employees use to further enhance the benefits of working with cloud services. The usage of these complementary services can help address gaps where the existing systems are inadequate. However, the use of such services by employees in environments that handle large volumes of confidential information can have consequences.

A survey conducted by Netskope (2021) revealed that 97% of cloud service apps used in enterprises are not approved by the IT department. These apps are also not subject to

the same type of management and are adopted by employees to supplement the usage of existing IT solutions. Furthermore, the study shows an increase in malware originating from these cloud services, with 67% of malware being found in cloud storage apps.

A study conducted in 2016 by the Institute of Information Security Professionals concluded that more than 40% of firms have little understanding of data privacy legislation and industry standards such as the General Data Protection Regulation (GDPR) (Institute of Information Security Professionals, 2016). Businesses must ensure that the apps and services they use comply with the norms and regulations. For example, cloud storage options may require the involvement of a third-party provider to handle data resources. The storage policies for this data need to be understood to prevent risks of data leakage and ensure proper storage of confidential information (TechTarget, 2019).

Organizations must be mindful of data security, as cloud infrastructures are vulnerable to hostile assaults and malicious actors. According to research conducted in 2019 by the Institute of Information Security Professionals, most cloud storage providers reported a data breach in the previous 12 months (Institute of Information Security Professionals, 2019). To guide the security of their cloud data, management must implement a security plan to address different types of cloud technology. This includes regular system upgrades and evaluations, access control and authentication mechanisms, and data encryption in transit and at rest (McAfee, 2020).

1.2 Intended Knowledge Contribution

1.2.1 Theoretical Contribution

The intended theoretical knowledge contribution of this study is to expand the literature on Shadow IT to encompass the increased usage of cloud services. While Shadow IT has been extensively researched and documented since the early stages of technological development, research into Shadow IT in cloud services is limited and not fully understood by researchers. Additionally, there is a lack of research on employees' perception and understanding of Shadow IT, as well as how IT managers handle Shadow IT in organisations. The theoretical contribution of this study will be to

examine the relationship between Shadow IT and cloud services, employees' perception of this relationship, and how these cloud services have impacted the understanding of Shadow IT. Furthermore, this study aims to contribute to the field of cloud computing and Shadow IT, building upon existing research, trends, and changes. It will draw upon existing literature, surveys, and semiconstructed interviews.

1.2.2 Practical Contribution

The practical contribution of this study lies in the knowledge that industry professionals and policymakers can gain from it. The findings can potentially aid in better decision-making, analysis of current structures regarding cloud computing and data privacy, and the usage of Shadow IT. It can also provide guidance on compliance with policies and identify areas for improvement in individual situations, ultimately leading to more efficient policies.

1.3 Research problem:

The adoption of cloud services has exponentially increased since its introduction, with Sweden leading in adoption rate in Europe. However, ensuring that businesses comply with policies and effectively utilize cloud technology remains a challenge.

One area of concern is the use of Cloud-Based Shadow IT by employees, which refers to the use of unapproved software and applications without the knowledge and control of the IT department. This thesis aims to explore the impact of employees' use of and managers' understanding of Cloud-Based Shadow IT on data privacy in the tech sector of Sweden. The research problem is formulated as follows:

Understand how Cloud-Based Shadow IT has been affecting employees' compliance with cloud services in the tech sector of Sweden.

1.4 Objective

This study examines the increased use of cloud computing by employees and the understanding of Cloud-Based Shadow IT by IT managers in the tech industry. It will identify the problems and possibilities associated with the usage of Cloud-Based Shadow IT through the current utilization of external and internal cloud services. The study aims to assist companies and IT managers in Sweden in making well-informed decisions in understanding and identifying the strengths, weaknesses, possibilities, and risks of Cloud-Based Shadow IT. The objective is to explore the relationship between Shadow IT and cloud services and how employees and IT managers adhere to and understand them. The research questions are as follows:

- *What is the understanding of the requirements regarding cloud services for employees and managers in the Swedish tech industry?*

- *What are the consequences of employees using cloud service solutions like Cloud-Based Shadow IT?*

- *Which factors are important for employees to understand and comply with the policies put in place?*

1.5 Limitations

This study limits to a specific sample size from the Swedish tech sector, because of this the study is limited to respondents which may have similar backgrounds. This can in turn affect the generalizable of the results when applied to other situations. The study's data is reported from participants experiences which may be subject to bias from unable to recall experiences or desirability. The scope of the study is also limited to Sweden which the results may not reflect to other countries. Academic literatures were limited to specific databases that could be accessed from the authors licences. Other literature, which could not be accessed could therefore not be incorporated.

2. Literature review

This chapter presents a literature review on Shadow IT and Cloud-Based Shadow IT, examining the current state of research and identifying existing gaps. It begins by explaining Shadow IT, Cloud-Based Shadow IT, goes into the literature and explores perspectives from both employees and managers.

2.1 Shadow IT

Shadow IT refers to the unauthorized use of IT resources by employees or departments within an organization, bypassing approval from the IT department to overcome deficiencies in existing IT systems. While Shadow IT can introduce new and more efficient ways of performing tasks for users, it also poses compliance and security risks (Gomez et al., 2022). Shadow IT is not a recent phenomenon but has existed since the advent of technology. With the increased adoption of technology in businesses, the prevalence of Shadow IT has also risen. Shadow IT refers to the unauthorized use of software and hardware within an organization, without official approval from management. It represents a problematic use of IT resources by different departments, creating security breaches and leaks of sensitive information. Various data breaches worldwide have been linked to the use of unauthorized software. In addition, Shadow IT has been present since the early days of technology, it has grown exponentially in the past decade due to the proliferation of cloud-based solutions. It is estimated that 20-50% of business departments operate IT solutions without approval from the IT department (Global Newswire, 2019). Additionally, up to 70% of employees rely on software that lacks approval (Capgemini, 2016). The numbers from the sources above give indications of the level of reliance on Shadow IT, it is important to note that the sources state different levels of it. However, it is a good indication of the interval that employees rely on Shadow IT

Research in information systems have increasingly been incorporating Shadow IT when dealing with IT governance (György et al. 2012). IT Governance is the guideline and framework to efficiently deal with the usage of information technology. It works by aligning the IT to firms' objectives (Calder, 2009). For Shadow IT there is challenges in finding approaches for IT governance that can measure issues and risks for the

phenomenon (Weill and Ross, 2004). User innovation is one these concerns from an IT governance point of view which can often be overlooked by management (Silic et al, 2016). Solutions from the bottom up of organisation tend to become more common, where IT departments have increased motives to work together with business units to address them (Chua and Storey, 2016). Moreover, providing proper governance over the user-driven innovations can help minimize the risks (György et al. 2012). Having this perspective in consideration can be of importance for organizations when dealing with Shadow IT.

Rentrop and Zimmermann (2012) emphasize the importance for organizations in their article "Shadow IT - Management and Control of Unofficial IT" that it is crucial for IT management to understand the irregularities that Shadow IT introduces to organizations. However, the authors note the lack of research on the topic and limited awareness of the consequences. Strong and Volkoff (2004) argue in their paper "A Roadmap for Enterprise System Implementation" that Shadow IT undermines and endangers the current systems in an organization, while also posing risks to official data flow. György et al. (2012) perceive Shadow IT as a security threat to businesses in their paper "Exploring the Shadows: IT Governance Approaches to User-Driven Innovation," stating that it hinders compliance with regulations at both organizational and national levels. Rentrop and Zimmermann (2012) also point out the absence of general frameworks or best practices, such as ITIL or COBIT, specifically addressing Shadow IT. The absence of frameworks can be seen as problematic in understanding the phenomenon of Shadow IT, however there are ways to dive into and dissect the parts.

A study of IT managers coined the term "50 Shades of Shadow IT" to illustrate the complexity and value of further categorizing this phenomenon (Smith & McKeen, 2011). Diving into these parts can be beneficial in understanding the phenomenon in more detail. One category that is brought up is End User Computation which refers to the use of approved software and services extended to areas that the IT department does not typically consider within the scope of the approved services (Zimmerman et al., 2017). This could include local departments developing approved development software further to expand its usage for their specific tasks. Secondly the usage of Workarounds that involve using a system for purposes other than those for which it was originally designed, utilizing the system's functionality while circumventing the requirements

imposed by the developers or the IT department for its use in the organization (Haag and Eckhardt, 2017) Another part is Personal IT that refers to the use of IT resources by individuals who have prior experience with a specific service for personal purposes. These individuals then employ the same service for business purposes, which may not align with the intended use defined by the service provider. Examples of personal IT include social media platforms, personal hardware, and private storage services (Haag and Eckhardt, 2017). Finally, Third-Party Access refers to external access that typically occurs when an employee agrees to work in a third-party environment to gather information from a business partner or client. This environment is not accessed through the employee's own organization and cannot be regulated (Zimmerman et al., 2017). Dividing the categorizations can be important in finding the usage and further understanding the phenomenon of Shadow IT. These factors are notable parts that are prevalent in the usage of shadow IT in today's environment where cloud services are increasing in workplaces

2.2 Cloud-Based Shadow IT

Cloud-Based Shadow IT or CBSIT is an extension of Shadow IT that primarily focuses on the use of unapproved cloud services by an organization's employees. (CBSIT will be used going forward). These services are used as alternatives to the organization's authorized cloud services. The motivation behind using a different cloud service is often the need for specific functionality to complete a task. Contacting the IT department and requesting approval can be a lengthy process that distracts from the immediate task at hand (Hulsebosch, 2016). CBSIT is a part of Shadow IT but not as recognizable as the literature established on Shadow IT as a whole. There are good reasons to separate the terms, as cloud services are today the main part of Shadow IT as more employees are turning towards its usage. There is still uncertainty in the literature as to what extent cloud services are used. One study conducted for a large enterprise noted that a total of 11,220 different cloud services were used in the organization, with only a mere 5% of the services being supported by the IT department (Anonymous, 2015B). Another paper noted that 86% of cloud services used in Fortune 1000 companies were not monitored or accepted by the IT departments (Ray 2016). Haag and Eckhardt, (2017) suggests that Personal IT and the use of cloud services by employees lead to teams avoiding the use

of internal IT, mentioning that entire departments can rely on them as a more efficient way of performing work tasks for their needs. Walterbusch et al., (2017) further argues that due to the easy accessibility of the cloud, employees will turn to finding solutions for their own needs when internal alternatives are not enough. Therefore, this can also mean that employees find the ease of setup of cloud computing solutions when they already have previous experience in them.

Cloud services in Shadow IT are noticeably rising at an alarming rate, yet the literature about it is sparse at best. Not recognizing the various factors contributing to the increased use provides limited help to employees and employers on how to address the issues that arise from it. In comparison, Shadow IT has extensive literature over an extended period, and organizations tend to have a general knowledge of it, even if it goes by another name. That CBSIT is becoming more popular in today's environment does have underlying reasons and there are explanations for its usage among cloud computing.

2.3 Cloud computing and the reason for usage in Shadow IT

Cloud computing involves the use of data transmission to deliver exceptional IT services by utilizing various service centres to store and manage data. There are numerous providers in the market that offer these centres for organizational use. Cloud computing enables companies to store their digital resources in a virtual network, managed by a provider, ensuring safety, storage, and access to the resources. Previously, digital resources were typically stored locally on a computer, but the introduction of cloud technology has simplified storage for businesses (Birje, 2017). Currently, there are three main categories of cloud technology provided by service providers: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Bhatti et al., 2018) (see Appendix for explanation).

The main reason employees rely on CBSIT is that existing cloud service solutions provided by an organization may not be sufficient for them to perform their work effectively. Instead, employees turn to different means that fulfil their requirements. This is usually motivated by the lack of communication and agreement between business departments and IT departments (Jones et al., 2004). While employees may use

the management-approved solution for IT systems, they help themselves by seeking additional solutions when needed, instead of relying on the IT department, to meet the requirements that the system cannot fulfil. The lack of appropriate education and awareness about the use of Shadow IT also drives this need forward (Puhakainen and Siponen, 2010). Researchers have attempted to understand the reasons why employees turn to Shadow IT solutions instead of internal ones. Some factors from these studies indicate that lack of communication plays a significant role for employees. Additionally, the decreased responsiveness of IT staff, lack of appropriate support, and understanding of the problem are also contributing factors (Campbell, 2005). The most common form of Shadow IT in the cloud industry is the use of SaaS programs, as they are easily accessible and can complement existing SaaS programs in the company. Most of these programs are available at no cost and are easy to learn. In many cases, employees usually have previous experience with these programs in their private lives (Haag and Eckhardt, 2017). Having employees turn to CBSIT is not without risk and while there may be comfort in using programs previous personal experience, there are security aspects to consider.

2.4 Shadow IT and its effects on Cloud Security

A survey conducted by Intel (2017) with 2,000 participants concluded that CBSIT has negative effects on cloud compliance. The survey revealed a link between CBSIT and its negative impact on cloud security, potentially compromising the secure storage of data. Since cloud companies have a vital role in ensuring that the data they collect adheres to legal regulations and agreements with customers, these findings raise concerns. The survey also highlighted the challenges IT managers face in analysing the use of Shadow IT in organizations, as there is no unified tool or framework to investigate the use of these services. In a study by Silic and Back (2014) that surveyed 3,000 IT managers, it was found that the most problematic issue with Shadow IT is that it exposes the internal network to malicious activity. Of the participants, 40% reported that the organization had experienced data integrity problems, and 25% mentioned that accounts had been hacked due to Shadow IT use. Walters (2013) states that if an employee stores data in a cloud-like environment brought in through a Shadow IT cloud solution, they risk violating legal policies, potentially causing further complications for a company. This opens the organization to legal problems that can affect the entire

organization. Gozman and Willcocks (2019) provide examples of how countries differ in their regulations: Germany, for example, does not allow personal data to be shared outside the country, while the UK allows personal data to be shared across borders if they are in the EEA, and France does not allow personal data to be shared across borders if the data is for foreign use. It is easy to see the potential security issues of sharing data with external parties based in other countries. Indeed, a few notable points about Shadow IT and Cloud Security are as follows:

• Data Breaches: Using a cloud service that does not have proper management approval may lead to data breaches beyond the control of the IT department. The service used may not have adequate security measures in place, and hackers can access data if information is leaked. The occurrence of these data breaches can also lead to problems with the cloud service provider, as they may view the client as untrustworthy and choose not to provide their service anymore (Walterbusch et al., 2017)

• Failure to Follow Regulations: Businesses risk facing legal action if employees use cloud services that do not comply with regulations or company policies. This can result in legal consequences, such as fines imposed by the government for non-compliance (Gozman & Willcocks, 2019).

• Data Control: When a company uses Shadow IT, the data is stored in a location where the organization does not have access, except for certain individuals. This lack of control over the data increases the risk of security breaches and compromises (Gozman & Willcocks, 2019).

2.5 Positive opportunities of using Shadow IT

While up to this point there has been a general negative view of Shadow IT, there are certainly positive opportunities that come with Shadow IT and its effects. The first positive aspect is that Shadow IT helps foster innovation within companies and enhances the way they manage their work by providing new solutions and alternative approaches for employees to tackle problems. It offers tools that can boost productivity, streamline processes, and improve customer experiences (Fuerstann & Rothe, 2014).

Secondly, Shadow IT provides increased flexibility for organizations, making it easier for businesses to adapt to changing demands and market dynamics. Unlike standard IT solutions, Shadow IT is not bound by rigid implementation processes, allowing employees to quickly provide better services and explore more agile options (Fuerstann & Rothe, 2014).

Thirdly, it offers resource savings for organizations. Instead of undergoing a lengthy process to implement a new IT solution, which can take months, Shadow IT already provides established solutions that employees can readily use. For example, an employee may utilize a free software tool to perform a task that would otherwise be unnecessary and costly for the organization to adopt on its own, considering its limited usage (Rentrop & Zimmermann, 2012).

The fourth opportunity presented by Shadow IT is that it increases employee motivation to perform their tasks. Shadow IT can offer more suitable tools that make tasks easier and more effective, leading to employees going the extra mile in their work. This reduces frustration with existing solutions and the prescribed methods of performing tasks (Rentrop & Zimmermann, 2012).

Finally, Shadow IT can foster collaboration among different departments within an organization by providing communication methods that may not be available through standard solutions (Rentrop & Zimmermann, 2012).

2.6 Employees' perspective on cloud services and Cloud-Based Shadow IT

From a employee’s point of view the shift to cloud services is widely recognized as having numerous benefits for firms, including easy setup, convenience, increased productivity, low operational costs, and improved collaboration. Data shared through cloud services can be accessed from anywhere, if an account is active, and an internet connection is available (Wafa'a & Khalid, 2020). However, companies often have doubts about the implementation process (Ya-Ching, 2019). The adoption of cloud services should be viewed similarly to the current mindset surrounding IT adoption. An important factor influencing employee adoption behaviours is understanding why cloud services are crucial for the company. Managers overseeing the adoption process play a

vital role in ensuring they communicate the reasons for adopting cloud services within the organization (Ali et al., 2020). There are however concerns that managers have for employees who wish to adopt more cloud alternatives.

Akande, Akinlolu, and April (2013) highlight in their paper "Management Issues with Cloud Computing" that managers are increasingly considering the adoption of cloud services due to their clear benefits. However, the authors note that these firms must understand that there are still several issues with cloud services that can be problematic from an employee perspective, potentially hindering adoption. Some key concerns mentioned by the authors include ethical issues, lack of standardization, potential security breaches, and dependence on external entities for data management. Bashari et al. (2017) touch upon these issues in their article "Cloud Computing Adoption: A Short Review of Issues and Challenges," suggesting that cloud services could lead to lower job satisfaction as certain job roles may be replaced by these services. Large organizations already operating cloud services may reduce the need for support jobs, technical engineers, and marketing staff, which can lower employee satisfaction with cloud adoption in the firm. Marston et al. (2011) argue in their paper "Cloud Computing — The Business Perspective. Decision Support Systems" that decreased satisfaction resulting from cloud service adoption can pose a threat to an organization's established IT culture.

Like the use of Shadow IT by employees, the motivation behind using CBSIT stems from a lack of suitable resources to complete tasks using existing services (Zimmermann and Rentrop, 2014). Cloud services provide employees with an easy-to-implement solution, offering free alternatives and user-friendly setups (Müller et al., 2015). Some employees also perceive it as a challenge to adhere to existing guidelines, considering them unreasonable, leading them to circumvent the guidelines due to a lack of value or disagreement (Behrens, 2009). Additionally, inadequate training on these guidelines can contribute to employees being unaware that they are not following established policies or understanding the concept of Shadow IT. The lack of training may also be driven by cost-saving measures within the organization (Silvius and Dols, 2012). From a management perspective, CBSIT is generally viewed negatively as it can lead to the misuse of secure information and potential breaches when dealing with these applications (Silic and Back, 2014).

2.7 Managers' perspective on cloud services and Cloud-Based Shadow IT

Managers have varying perspective of how to deal with CBSIT in today's environment. A notable study by ReRez Research (2012) reported that one out of five IT managers felt that employees lacked awareness that Shadow IT contradicts IT policies and security compliance. However, the study also revealed that four out of five employees were aware that using non-approved IT services could compromise security and violate compliance regulations. Another study conducted by Nasuni, which surveyed 1300 employees, showed that one-fifth of them used Dropbox to store company information, despite half of the participants recognizing that this went against company policies (Nasuni 2013). Walters (2013) discussed the challenges faced by managers or CIOs in managing data from these services when data is shared through cloud services. The author mentioned that storage cloud options like Dropbox and Google Drive are often used to store sensitive information, while Office 365 and Google Apps are utilized for collaboration on shared documents. The main issue highlighted for managers and CIOs is that employees use personal IT accounts to access these services, leading to data retention challenges when employees leave the organization (Lewis, 2016). Organizations bear the responsibility for all data stored in different cloud providers, as outsourcing the data does not absolve them of accountability (Géczy et al, 2011). According to Walters (2013), this underscores the need for education within organizations to establish best practices.

2.7.1 Types of Cloud-Based Shadow IT

There are various types of cloud-based services that employees use without being aware that they are considered Shadow IT. This part will cover some of the most common types of cloud-based services that are used (Nasuni, 2012). The services are some of the more popular examples on the market today which employees use because of previous personal experience with them (IBM, 2023). Moreover, CIOs in companies are increasingly worried about usage of cloud services that employ document sharing options or productivity suites. A few examples of these are Dropbox, Google Drive, Google Apps and Office 365. The worry stems from the increased risk of sharing and discussing sensitive information with the risk of it being exposed (Walters, 2013). From

the perceived problems of CBSIT a few notable types of collaboration services are presented below that are popular in workplaces:

Service	Type of service
Dropbox	Cloud based storage service
iCloud	Cloud based storage service
Google Drive	Cloud based storage service
OneDrive	Cloud based storage service
Mega	Cloud based storage service
Trello	Cloud based communication service
Slack	Cloud based communication service
Zoom	Cloud based communication service

Table 1: Types of CBSIT (techadvisor 2023), (techradar 2023)

2.8 The challenges of cloud computing

The rise of cloud computing has brought forth issues and challenges that organizations increasingly face. To successfully adapt to and implement cloud computing, organizations need to be aware of these challenges and understand their implications. Gaining a thorough understanding of these challenges can help prevent future risks and issues.

2.8.1 Security and privacy

Cloud computing offers the ability to back up and store valuable resources in a digital environment, potentially enhancing data security. However, it can also have the opposite effect. If a service provider experiences a breach, it can impact not only the provider but also its clients, potentially resulting in service unavailability and data leakage. Service providers employ security applications, encryption technologies, data loss prevention programs, and system monitoring to mitigate these risks. However, it is important to recognize that these systems are not fool proof (Panigrahi, Ghose & Moumita, 2013). Another issue raised with cloud computing is the potential for service providers to collect and store shared data, which can compromise the confidentiality of sensitive information (VasanthaAzhagu and Gnanasekar, 2016). Organizations consider

this a significant issue when deciding to adopt new cloud services, emphasizing the need for proper data privacy systems in place (Shahzad, 2014). The design of cloud services allows hackers, in the event of a security breach, to potentially access multiple account details (VasanthaAzhagu and Gnanasekar, 2016). An example of such an attack occurred in 2014 when hackers compromised millions of account login details and photos from Dropbox and iCloud (Salcedo, 2014).

2.8.2 Compliance and policy making

Compliance is a term that varies in its definition across the literature, making it difficult to provide a single definition. In this essay, the definition by Fernandez and Yiman (2016) will be used. The authors define compliance as the enforcement of regulations and rules that are outlined in an organization's policies. These rules may originate from governments, organizations, or the company itself. The literature shows the importance of policy making for firms dealing with cloud services and sharing personal information with these services (Chua, Herbland, Wong, and Chang, 2017). Having knowledge and understanding of the risks greatly increases awareness about the security risks and potential implications when using external services (Milne and Culnan, 2004). As outsourcing services to companies are increasingly becoming more regulated, transparency in data handled in organizations is of more importance (Outsourcing Law, 2017). This means that practices involving outsourced services to other companies are being more controlled in today's environment and policy making. However, for the cloud, this factor of regulation is less prevalent when data is handled in the cloud (Seddon and Currie, 2013). Regarding shaping IT policy, the IT departments have good control over hardware and software usage in the organization. With it, they help shape the policies in use in organizations, including the usage of third-party options. In cloud services, however, this perspective is somewhat neglected where an unawareness of the services that are set up is not accounted for (BT, 2015). The nature of SaaS cloud applications, being cheap, easy to set up, and convenient, allows the introduction of a service without following up on best practices regarding policies. Furthermore, employees who seek to follow deadlines for work tasks and are pressured are more likely to avoid policies to hit targets (Gozman & Willcocks, 2019).

2.8.3 Challenges of turning to cloud computing

Calculating the cost of cloud computing for businesses that implement them can be difficult because it can be charged based on the demand the business has. Therefore, it brings challenges to budgeting and planning. There are also various providers, which can result in difficult decision making when choosing the right company (Panigrahi, Ghose & Moumita, 2013). Another challenge today is that some providers set up lengthy lock-in periods, meaning companies can be stuck with a plan that is not suitable for them. It is important to push for cloud service providers to have flexible plans that require no lock-in period. The switch should also be handled with ease and consume less time (Panigrahi, Ghose & Moumita, 2013). There is also the problem of companies becoming too dependent on the services to help and keep the applications up (Gozman & Willcocks, 2019). Today, some providers do not offer 24-hour support to their customers, which can lead to downtime of the services that cannot be fixed until support is available again. Businesses need to evaluate the service provided and its format to make decisions when implementing a cloud provider (Panigrahi, Ghose & Moumita, 2013). One challenge organization face when dealing with cloud providers is the increasing cost depending on the amount of data the servers are handling. This results in high bandwidth costs for companies that have complex applications running. This can be off-putting for companies that do not have the available resources. Companies need to consider this in their plan and evaluate if they can allocate the necessary resources (Panigrahi, Ghose & Moumita, 2013).

2.9 Data Storage

In the last decade, the collection of data has steadily increased, along with the awareness of the potential privacy risks of data collection. Models that depend on users' data have gained various new implications for businesses, such as using data to generate content, ads, influence decision making, and analyse business needs. This has set a new standard for businesses to operate with. However, with this increased trust from customers about the handling of their data, issues of trust have also become more relevant. These issues have gained momentum from various data breaches that have gained attention around the world (Kleindienst, 2017). Sweden has long had an interest in preserving the integrity of its citizens and was the world's first country to implement measures to adopt

data protection in its 1973 Swedish Data Act. It served as a starting point for a law ensuring permits for the processing of personal data. In practice, it meant that companies seeking to collect personal information about a Swedish citizen needed to apply for licenses from the Swedish Data Protection Authority. Since the implementation, various changes to data privacy laws in Sweden have been put in place, but one notable law, the GDPR, has introduced new measures to be dealt with (Wikin & Sjöblom, 2022).

2.10 The General Data Protection Regulation (GDPR)

The GDPR is a regulation introduced for member countries in the European Union that came into effect in 2018. The regulation is used to protect citizens with new measures to ensure control of data collection and data protection. It applies to all businesses that collect individual data in the EU and applies to organizations that operate outside the EU. There are some main points that businesses need to adhere to comply with the GDPR (Zhou, Barati & Shafiq, 2023):

Collection: Data that is collected can only be used for specific stated purposes, which need to be informed to the person it is gathered from (Zhou, Barati & Shafiq, 2023).
Consent: The data collected must have been accepted from the individual beforehand, with a clear purpose (Zhou, Barati & Shafiq, 2023).
Accountability: Organizations must have measures to ensure they are in line with the GDPR and that the data they have collected is accurate (Zhou, Barati & Shafiq, 2023).
Data Storage: Organizations cannot keep the data longer than stated to the individual and longer than required for the intended purpose (Zhou, Barati & Shafiq, 2023).
Data Security: Organizations need to take measures to keep the data protected and confidential (Zhou, Barati & Shafiq, 2023).

3. Method

In the following chapter, the research design and data collection methods are described. The chapter presents the rationale behind the data collection and explains how the analysis is performed. The reliability and validity of both data collection methods are discussed, along with ethical considerations in conducting the research.

3.1 Research Strategy

When choosing the research strategy for the study, philosophical considerations are considered to determine the most appropriate design. Epistemology, a branch of philosophy that explores the nature of knowledge and the conclusions that can be drawn from it, informs the selection of research methods. Epistemology is typically categorized into three main areas of research. The first one is Positivism, which deals with knowledge derived from primarily quantitative data. It emphasizes observations and measurements as key factors in drawing conclusions from data. The second area is Interpretivism, which is mainly used in qualitative research. It posits that data is contextualized and relies on individuals' experiences to gain insight into the motives and thoughts underlying their experiences. The third option is Postmodernism, which holds that knowledge is inconsistent. To address this, knowledge needs to be further broken down to encompass diverse perspectives and experiences (Bryman and Bell, 2019). This thesis adopts a combination of Interpretivism approach. The study analyses quantitative data to draw indications and conclusions based on key factors. Focusing on the underlying factors behind the answers rather than traditional facts. The quantitative data is used to shape the questions for the qualitative interviews. The use of the method also allows for replicated results, statistical analysis and objectivity. It also incorporates qualitative data to capture individuals' experiences, identify themes, and draw conclusions. This combination allows for a deeper understanding of the research questions and the study's objectives (Schoonenboom & Johnson, 2017). Interpretivism approach is most common in qualitative methods, but it does not reject the quantitative method and the knowledge it can generate.

The study also takes an inductive approach, using data to identify themes, patterns, and relationships, which can then be used to generalize the results and gain a deeper

understanding of the phenomenon being studied (Creswell, 2014). In this study, an inductive approach will be employed to gain insights into employees' and IT managers' experiences of CBSIT. The inductive approach is beneficial in that it enables understanding from current theoretical frameworks to gather new understandings and insights.

The proposed method for this study is divided into three parts. The first part involves conducting a literature review to examine existing research on cloud technology and data privacy. The second part consists of a survey targeting industry professionals in cloud computing who have day-to-day experience with cloud work tasks. The final part involves conducting interviews with IT managers about the use of Shadow IT in their organizations. The data collected will be used to understand how employees perceive the use of Shadow IT in cloud-based organizations. A mixed method approach is the use of combining multiple research methods, which can be quantitative and qualitative data (Schoonenboom & Johnson, 2017). The mixed method approach was found appropriate for the study because it focuses on two groups, employees, and IT-managers. Having the purpose to ensure that employees and IT-managers make well-informed decisions, a mixed method approach leads to rich insights and deeper understanding. It can capture the problems from employees and through the interviews help explain them further with the help of the IT-managers experiences.

3.2 Research design

This research uses a case study for its design, the case in question is the phenomenon of CBSIT. A case study is the use of examining individuals, groups, events or phenomena to analyse and find underlying patterns. With the use in gathering information to achieve generalizable results. The downside is that case studies tend to be focused on the specific matter and can in turn be hard to make generalizable findings. There are however positivise that is allows for new insights into a limit area. For this study where CBSIT is limited, the use is motivated with the information it can generate using a case study. The study follows an explorative approach to generate knowledge about an area with limited existing research in the given context. An explorative study aims to gather information on broadly defined terms (Creswell, 2018).

3.3 Literature selection

The literature selection for the study was performed through Linköpings University Unisearch database, The Unisearch database gives access to hundreds of databases for student at Linköping University like Scopus, ScienceDirect, Sage Journals and Web of Science. The motivation behind using Unisearch was because of the high standard for databases selections, being a university database ensure access to academic material and having variety of publishers. Unisearch considerations were made of how the field of the database is related to information systems, if articles are peer-reviewed and if the journals cite earlier sources in the area. AIS eLibrary was also used for searching for journals, which is a database of information systems research. There were however some issues with licensing for this webpage, which limited access to some journal articles.

The terms that were used in the search were the key words for this study: Cloud-Based Shadow IT, Shadow IT, Swedish Tech Sector, Data Privacy, Managers, Employees, End User Computation, Workaround, Personal IT, Third-Party Access. Other words for Shadow IT such as Grey IT, Stealth IT, Rogue IT etc were used to find similar papers. In turn the papers that they were cited by the articles were looked at to find extended literature from the articles that the authors had cited. The papers that were gathered were mainly peer-reviewed articles to ensure high quality standards, white papers also occurred and relevant articles when ensured they had proper sources backing them.

3.4 Mixed Method Approach

A mixed method approach involves using both quantitative and qualitative research methods in a study. It is employed when one approach alone does not provide sufficient information for the researcher. By combining both methods, a study can yield increased knowledge about a phenomenon and provide a more comprehensive explanation of the results. Incorporating different perspectives can lead to better conclusions, depending on the study. The goal of a mixed method approach is to strengthen the conclusions of the research question, aiming for higher validity of the study and the knowledge generated from it (Schoonenboom & Johnson, 2017). The assumption is that the results from both types of data collection will enable a more detailed understanding of the problem

(Creswell, 2018). In this study, a mixed method design is motivated by the need to investigate employees' perceptions of IT. Including IT managers in the qualitative study can provide insights into the relationship between employees and Shadow IT within an organization. It can also shed light on why employees turn to Shadow IT and how IT managers view its usage.

The mixed method design includes both quantitative and qualitative data. The research starts with a quantitative survey to capture employees' perceptions of Shadow IT. The survey results will inform the questions asked to IT managers, building upon the employees' perspectives. This study design assumes that it may help IT managers gain a wider perspective on the problem and encourage them to be open about their own experiences.

3.5 Methods for Data Collection

The study was conducted in two parts. The first part involved a survey administered to employees, with the survey questions based on the themes identified in the literature review and standard survey methodology. The survey responses were analysed to develop semi-structured interviews with IT managers. Both datasets were analysed separately, and no individuals from one method were included in the other (Creswell, 2018).

3.6.1 Sampling

Respondents for this study were gathered through contact with various companies in the tech sector to collect data for both the quantitative and qualitative research. Participants were contacted via email provided on the company's website to express interest in participating in both the quantitative and qualitative studies. Several important factors were considered when selecting participants. Firstly, individuals with mutual connections to the researcher were excluded. This was done to minimize potential bias in the participants' responses due to shared interests or relationships (Bryman & Bell, 2014). Secondly, participants were required to work in roles that involved using cloud services in their everyday tasks, ensuring relevance to the study. Finally, participants needed to be affiliated with Swedish companies in the tech industry that utilized cloud

services. The companies where the participants worked were examined before reaching out for the questionnaire.

3.7 Survey

The research first takes a quantitative approach to explore the relationship between employee behaviour when engaging with cloud services in their everyday tasks. Quantitative research involves the use of numerical factors to search for generalizable results that can be used to measure a population. An objective standpoint is sought after to make predictions about certain relationships, patterns, or trends among the test group. It can be used to test hypotheses, test existing theories, or build towards a qualitative approach. There are both positive and negative aspects of quantitative research that need to be considered when deciding to use this method (Creswell, 2018). Using quantitative research can make it easier to provide standardized results in the collected data and help generalize the findings. The findings can therefore be assumed to be repeated in a future study if the prerequisites are similar. It can also produce results that can be compared to other groups, settings, and times to analyse and compare the findings. However, quantitative research also has negative aspects that depend on the motivation of the research. The results may not capture the reality of the participants if the research explores too complex subjects. The chosen measurements may not be the right ones to explore, as other critical factors that influence the results are ignored. Quantitative research is also prone to structural bias, missing relevant data, not using the appropriate sampling method, and improper measurement, all of which can lead to incorrect conclusions. Finally, the lack of context in a setting can mislead the results, where, for example, a recent trend may have affected the participants' answers, which may not hold true in the future (Bryman & Bell, 2014).

3.7.1 Survey Guide

The survey was designed with recognition of the guide from Granello and Wheaton (2004) to establish a solid foundation for the design. Google Forms was used for its easy design and familiarity among participants. At the start of the survey, an introduction was provided, giving information about the research and its purpose. It included the name of the researcher, university, and details on how the responses would

be used and handled. These steps were taken to make the survey transparent for the respondents regarding their participation. Considering that the survey was conducted online, efforts were made to address respondents' potential reluctance to answer online surveys (Dillman, Smyth & Christian, 2014). Online surveys can sometimes be perceived as annoying and unwanted, especially if there is a lack of interest in the topic. To mitigate this, the sample consisted of workers in the tech sector who, to some degree, might understand the topic. Additionally, emphasis was placed on the survey's design.

The layout of the study was divided into four parts. The first part consisted of general questions about the participants, ensuring their confidentiality (Noordgard, 2011). Information about gender, age, and experience in the tech sector was collected. The second part delved into the employees' current usage of cloud services in the workplace and their issues with such usage. The third part presented external cloud services, and employees were asked about their usage of these services in their work. Finally, the last part focused on Shadow IT and data handling. The questions examined the usage of current cloud services in the workplace and their impact on Shadow IT. It also explored why employees use Shadow IT and investigated their understanding of its use. The survey also inquired about employees' comprehension of organizational policies and their approach to them.

The survey questions included various types, such as how questions and statements that respondents could agree or disagree with. The statement questions or agree/disagree method aimed to prompt respondents to reflect on their own experiences and indicate their level of agreement. The survey was completed by 30 anonymous respondents who were invited via email. The email gave information about the survey, what it meant to partake and what their information was used for. Companies were contacted through the website www.techsverige.se a member organization of companies in the tech sector in Sweden. Techsverige has 1450 member organizations with around 100 000 employees in total. TechSverige strives to create the best opportunities for tech companies to be competitive. They are also a part of Svenskt Näringsliv which is the top organisation for enterprises in Sweden (TechSverige 2023) The website was chosen for its ease of use in reaching participants, having lists of all their members with contact information and because of its reputation as a trustworthy member organization.

3.7.2 Survey Questions

The following table presents the survey questions, the division of survey parts, and the literature from which the questions were derived.

Part 1	**Information about participant**	Question based on literature
Q1	What is your gender?	Swift et al, (2015)
Q2	What age are you?	Gigliotti & Dietcsh, (2014)
Q3	How many years of experience do you have in the IT-sector?	
Part 2	**Cloud Based IT- Services**	
Q4	How frequently do you use Cloud-Based IT services in your work tasks?	Netskope (2021), Global newswire (2019), Capgemini (2016)
Q5	How easy is it to access and use the cloud services provided by your company?	Birje (2017), Lowe (2015), Haag and Eckhardt (2017)
Q6	How strongly do you agree with the statement “I am satisfied with the current Cloud-Based IT services in my workplace”?	Lowe (2015)
Q7	How strongly do you agree with the statement "The Cloud-Based IT services provided in my workplace fulfil the requirements for my work tasks"?	Jones et al., (2004), Zimmermann and Rentrop (2014).
Q8	How strongly do you agree with the statement "I can easily get help with the Cloud-Based IT services from my IT department"?	Hulsebosch (2016), Puhakainen and Siponen (2010)
Part 3	**Questions about Cloud-Based Shadow IT**	
Q9	How often do you use cloud services for work purposes that are not officially approved or provided by your company (e.g., personal Google drive account)?”	Ray (2016),
Q10	Have you used any of these services in your work tasks? (one or more)	Nasuni (2013), Walters (2013),
Q11	How comfortable are you with using the above services for work-related tasks?	Müller et al., (2015)
Q12	Do you consider these services a good addition in your everyday work tasks?	Müller et al., (2015)
Q13	How strongly do you agree with the statement, "I have needed to use these services because of insufficient IT solutions"?	Jones et al., (2004)

Q14	What factors influence your decision in using these services for work purposes? (one or more)"	Rentrop & Zimmermann (2012), Gomez et al 2022), Hulsebosch (2016), Lowe (2015)
Q15	If other option, please state the reason	
Q16	Are you familiar with the company's policies around the use of these services for work-related tasks?	Nasuni (2013), TechTarget, (2019), Gozman & Willcocks (2019), (Silvius and Dols, 2012), Gozman & Willcocks (2019)
Part 4	**Cloud-Based Shadow IT**	
Q17	How familiar are you with the concept of Cloud-Based Shadow IT?"	Silvius and Dols, (2012)
Q18	Results survey question 18: "How strongly do you agree with the statement "I think my IT department educates me about the use of external based IT cloud services and the implications they bring"?"	Puhakainen and Siponen (2010), Walters (2013),
Q19	How strongly do you agree with the statement, "When using these services, I make sure to think about the information I'm sharing"?	Gozman & Willcocks (2019), (Chua, Herbland, Wong, and Chang 2017), Silic & Back (2014)
Q20	Have you ever experienced a data breach or security incident because of any of these services in the workplace?	Institute of Information Security Professionals, (2019), Walters (2013, (Kleindienst 2017)

Table 2: Quantitative questionnaire

3.7.3 Critical Review

The usage of the approach in this quantitative research may not yield standardized results for the whole population because of the use of respondents from a specific sector. Different types of employees in cloud companies are examined, which can provide different opinions based on their own roles and work tasks. It is also not limited to a single organization but includes different ones. If the study were focused on a single set of data, the results could be used for decision-making within that specific company. However, this study is not motivated by that objective. Instead, it aims to find standardization and further explore this through qualitative research. The results of the study are open to bias because employees may not fully understand the usage of the services and may feel the need to protect their own interests within the company. Reaching out to individuals through email can also introduce bias, as employees may

form a perception of the person sending the survey before participating (Dillman et al., 2014).

3.8 Method of analysing Survey Data

The method of analysing the survey data first involves collecting and summarizing the gathered data. Google Forms and tables were used to create appropriate charts for the data, and the answers were categorized into different themes. The analysis of the survey data and visualization can be found in the results chapter, along with a description of the work done. The data was further broken down through descriptive analysis to find the mean, median, mode and standard deviation of the answers. This was done to simplify the data description and facilitate further analysis related to the literature (Nordgaard, 2011). Having these measures help give an understanding behind the answers and can make further analysis. Moreover, a confidence interval is used for the analysis. A confidence interval is a tool that helps look at degrees of uncertainty in data sets based on samples, it gives a probability that an answer falls between certain values from the mean. The most common probability levels are 95% and 99% confidence level (Wienclaw, 2021). In this study the data was set up with 95 % percent interval using the formula:

$$\bar{x} \pm (Z * (s / \sqrt{n}))$$

X = mean
Z = desired confidence level
S = standard deviation
n = sample size

Figure 1: Confidence Interval Formula

The survey analysis from the data used to identify themes from the responses and explore employees' perceptions, aiming to find underlying patterns in the responses. In addition, the literature was discussed in comparison to the findings.

3.8.1 Reliability and Validity for Quantitative Method

Reliability in a study refers to how trustworthy the results are, considering factors such as data collection and analysis. It describes the consistency of results when compared to another study under similar conditions. Having high reliability shows that the results can be increasingly trustworthy among academic literature. To achieve high reliability, researchers should maintain consistency in data collection methods, standardize research conditions, and provide equal information to participants (Höst et al., 2006). In this study, high reliability was pursued by reviewing existing literature in the field and similar areas before conducting the study. Clear information about the study's purpose was provided to participants, and careful consideration was given to whom the invitations were sent (Nordgaard, 2011). Reliability was as well calculated with the Cronbach's alpha coefficient which is a method that measure internal consistency within statistical methods. It measures the way that a test is exploring the concept that is presented. Where it gives an answer to the similarity in the relation of the observations. The method is one alternative to measure the rate of reliability of a quantitative test. For this study Cronbach's alpha coefficient was used to determine the internal consistency between the different parts of the quantitative study where a Likert scale was used. A Likert scale is a rating method of several option of answers, either 5 or 7. In this study the Likert scale a 7-poing scale was used. The formula for calculating Cronbach's alpha coefficient is as follows:

$$\alpha = \frac{N * \overline{c}}{\overline{v} + (N - 1) * \overline{c}}$$

Figure 2: Cronbach's alpha coefficient formula (Cronbach, 1951)

N = number of test subjects

$\overline{v}$ = Mean variance between subjects

$\overline{c}$ = Mean variance between questions

Cronbach's alpha	**Internal consistency**
$\alpha \geq 0.9$	Excellent
$\alpha > 0.9 \geq 0.8$	Good
$\alpha > 0.8 \geq 0.7$	Acceptable
$\alpha > 0.7 \geq 0.6$	Questionable
$\alpha > 0.6 \geq 0.5$	Poor
$0.5 > \alpha$	Unacceptable

Table 3: Cronbach's alpha coefficient scale of internal consisteny (Cronbach, 1951)

Validity involves accurately measuring what the study seeks to accomplish. High validity ensures that the results align with the study's objectives and provide an accurate representation of the phenomena under investigation. To enhance validity, researchers can consider variations in the research, potential effects of data collection methods on results, and the formulation of questions to minimize variations. Appropriate data collection methods should also be employed (Höst et al., 2006). Internal and external validity are also important factor to consider in quantitative studies. Internal validity looks at if the results obtained is not affected by other factors while external looks at the degree that the results can be generalized to different settings (Straub, Gefen & Boudreau, 2005) For this study examples of threats to internal validity that could happen is using a single group study, social threats, attrition, and history (Dillman, Smyth & Christian, 2014). First having a single group study being the tech sector for example give results in biased assumptions or confusion among questionnaires. Secondly social threats were considered where respondents behave differently in accordance when the results can affect them. Attrition is a threat were respondents leave the research, meaning that the research only considers those who are left. Finally, history can be a threat where historical events of a phenomenon can affect their answer, for example politics, media recognition or regulations (Andrade, 2018). Examples of external validity threats for the study is sample selection bias where the sample is not capturing the population. Observer bias is another which is when a respondent knows they are being observed and alters their answers. Moreover, the situation effect can affect a respondent where setting, time, researcher, and location can alter the opinions (Andrade, 2018).

High validity was sought after in this study by using standardized questions which was sought after to be formulated in a way that facilitate easy participant responses. The questionnaire was established based on existing literature on the study topic which would give it good grounding. Using clear communication with the respondents before and during the survey ensured consistency with the information they received. Companies were selected randomly within the tech sector, and personal considerations were not utilized. The respondents were also made aware of the anonymity in participating in the study. Overall, high validity was sought after by ensuring good methodology, research of existing literature, observing variation of results and relevant data collection method.

3.9 Semi-Structured Interviews

The second part of the research process involves conducting semi-structured interviews with IT managers in the tech industry who have knowledge about cloud services. The goal is to understand the perceived usage of cloud services considered Shadow IT in their organizations. The interviews explore awareness, reactions, and the impact on their work when they recognize the presence of Shadow IT. Five IT managers from different tech sector companies in Sweden were interviewed. They were contacted via email through "TechSverige," and the managers were selected randomly from the companies listed on the site. The interviews were help in Swedish and took place via teams with the length of around 20-30 minutes for each interview.

Semi-structured interviews are a qualitative research method that uses open-ended questions to participants, aiming to capture a broad range of experiences. It enables a discussion format where the participant provides the sought-after answers in a less formal manner. The researchers do not follow a set list of questions; instead, the questions asked can vary to capture the desired results. For example, some prepared questions may not be used if previous answers or experiences have already addressed the topic (Creswell, 2014). Semi-structured interviews allow for a lower level of formality, which can help elicit experiences that might not emerge in a more formal setting. The advantages of semi-structured interviews include facilitating detailed and explanatory information through two-way communication. It also allows the

interviewee to gradually open, creating a more personalized experience that flows naturally (Bryman & Bell, 2019). However, disadvantages include increased time consumption compared to other methods and the possibility of conversations straying off-topic, resulting in irrelevant information for the research. Lack of uniformity among participants may introduce biased opinions, as some questions may not be asked due to previous answers. Additionally, analysing the questions can lead to misinterpretation of answers, as understanding them accurately can be challenging, potentially resulting in interpretations that differ from the respondents' intended opinions (Creswell, 2014).

3.9.1 Qualitative Research Design

Qualitative research design seeks answers to complex phenomena using non-numerical data to gain detailed experiences, opinions, and understanding of concepts. It is often challenging to generalize and standardize qualitative research for the entire population, unlike quantitative research. However, the results generated can provide insights for further research and understanding of a topic. Like quantitative research, qualitative research is prone to bias due to researchers' filtering of information, potentially missing important details. Participants' biases can also influence their answers based on their experiences, leading to explanations that protect their own interests and opinions, which may not align with reality (Saldaña, 2015).

3.9.2 Method of analysing Interview Data

The analysis of the semi-structured interviews utilizes Litchman's (2013) approach, which involves three C's: codes, categories, and concepts. Firstly, the answers from the interviews were coded through transcriptions and audio recordings. Next, the answers were categorized into themes and further divided into concepts. Thematic analysis was then conducted to identify patterns and themes within the answers. Thematic analysis involves coding the transcripts to identify key words or sentences that provide insight into participants' experiences. By applying this process to each transcript, similarities and themes can be identified, leading to ideas and conclusions that help contextualize the phenomenon under investigation (Bryman & Bell, 2019). For the interviews the transcript was translated to English and analysed to find similar patterns between the interviews as well as finding reoccurring themes.

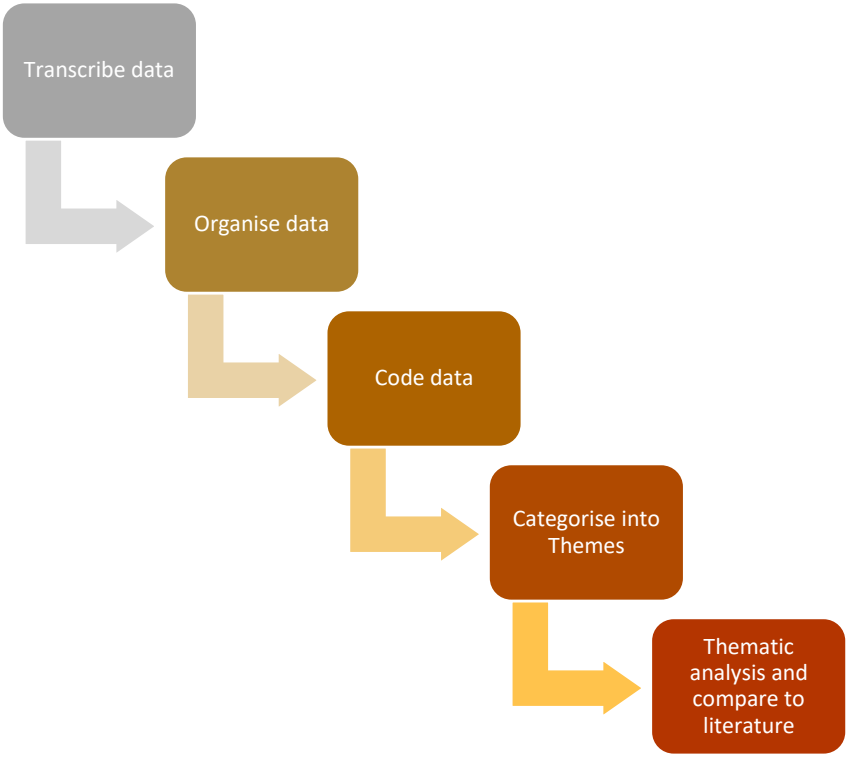

Figure 3: Description of qualitative analysis

3.9.3 Reliability and Validity for Qualitative Method

While reliability and validity are commonly associated with quantitative research, they are also important in qualitative methods. To ensure reliability in qualitative data, it is necessary to establish that the data is dependable and can be replicated by other researchers conducting similar studies. Confirmability of the data is another method, ensuring that the data collected are free from biased opinions and accurately capture the experiences of the participants. Lastly, transferability is a common method, ensuring that the gathered data can be applied to find similar findings in different situations and populations. For validity, the data should be credible, ensuring that the findings are realistic and precise. Similarly, the data should be transferable to other findings and confirmable as reliable, without bias (Morse et al., 2002).

In this study, reliability and validity have been considered in several ways to strengthen the collected data. Firstly, the research design is discussed, highlighting the philosophical grounding in selecting the method. Secondly, a mixed methods approach

is used instead of a singular approach, allowing for a more in-depth understanding of the research topic and obtaining different perspectives on the problem. Thirdly, the literature review strengthens and supports the findings, acknowledging similarities with what other researchers have gathered. By utilizing existing knowledge in the field, the study aims to contribute to future research. Finally, the use of an exploratory study can provide further insights in a relatively small field and guide future research (Schoonenboom, 2017). These factors were looked upon for the study to increase the trustworthiness of the results and help make the insights more in-depth. Having the questions be based on the survey and literature helped create a discussion with the respondents where they could feel free to express their experiences.

3.10 Ethical Considerations

Participants in both the quantitative and qualitative surveys were informed about the study's objectives, the use of data, and the guarantee of anonymity. They were informed beforehand in the email and as well in the survey and interview. The participants were also made aware of having the opportunity to end the survey or interview at any point. To ensure participant privacy, the interviews focused on general questions rather than personal information. All recordings were deleted once the transcription and coding processes were completed. The participants also had the opportunity to verify the results afterwards and adjust the answers if necessary. The selection process for data collection avoided any connection between the author and the participants to minimize potential bias. Google Forms was chosen as the survey platform due to its familiarity and ease of access for participants.

4. Results from Quantitative study

In this chapter, the empirical data is written out in accordance with the method presented in the method chapter. The data is used to state the findings and experiences of the respondents of the Survey. A total of 30 respondents undertook the survey from the Swedish tech sector. The questions ranging from 1-7 are based on the grading word in the question. An example is the word often with 1 being not very often, 4 is neutral and 7 is very often.

4.1 Part 1: Information about participant

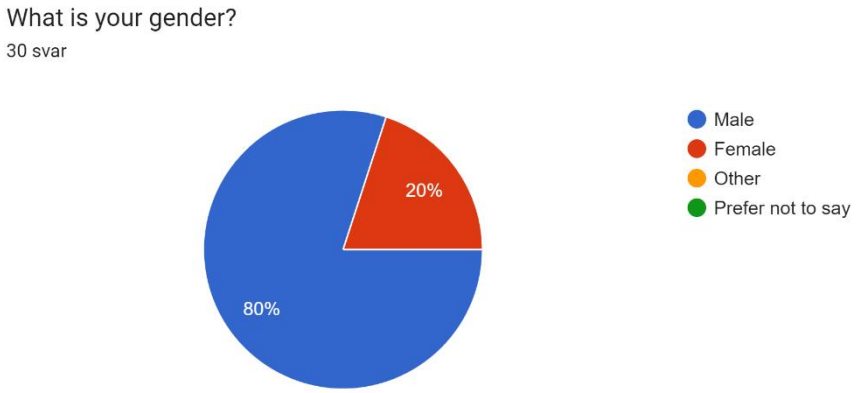

Figure 4 : Results survey question 1: “What is your gender?”

Figure 4 is based on the first question of the survey regarding the gender of the participants. The chart describes that most respondents, 80%, were males, while 20% were females. No respondent selected the option “Other” or “Prefer not to say”.

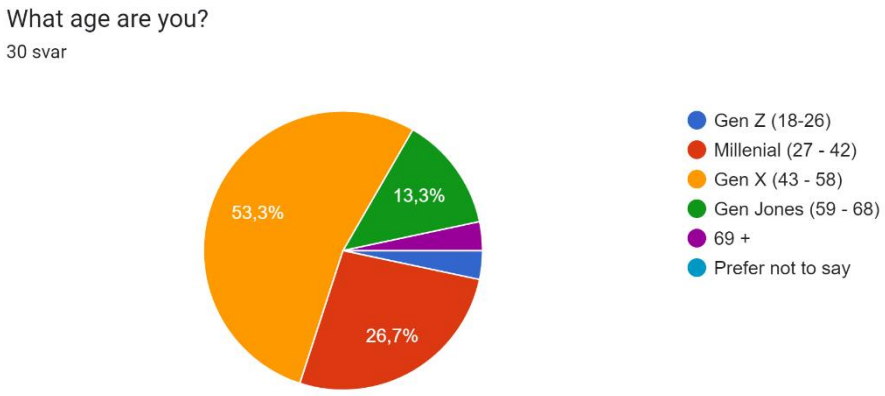

Figure 5: Results survey question 2: “What age are you?”

In Figure 5, respondents were asked to choose their age group, which was based on generational sorting. Respondents of all age groups participated in this study with a majority being in the Gen X (43-58) group. The millennial group came after with 26,7 % of participants. After that Gen Jones with 13.3%. Lastly Gen Z and the group 69 had each 10 % of the total number of respondents. None of the respondents chose the alternative "Prefer not to say."

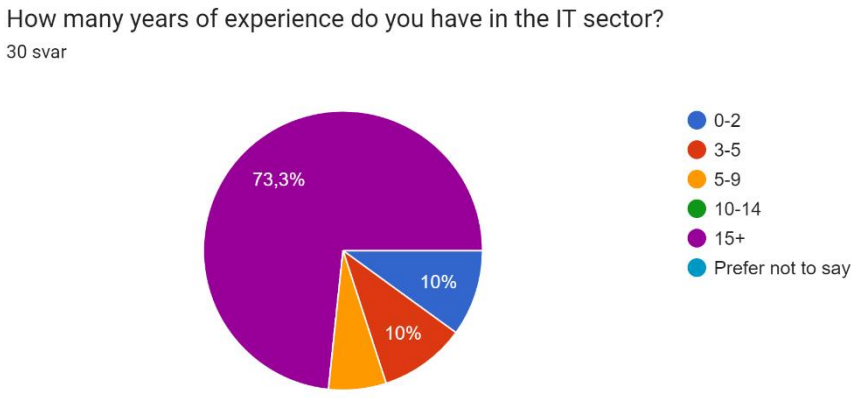

Figure 6: Results survey question 3: “How many years of experience do you have in the IT-sector?”

Figure 6 represents the years of experience of the participants in the IT sector. The groups were presented in different experience spans. The group with the highest

percentage was those with 15+ experience accounting for 73,3 % of respondents. The option 3-5 years and 0-2 years both had 10 % of respondent each. Finally, the option 5-9 years accounted for 6,7 %. No respondent selected the group 10-14 years and the option “Prefer not to say” It shows that most of the respondents who participated in the survey have extensive experience in the sector, with 73,3% having worked in the industry for over 15 years.

4.2 Part 2: Cloud Based IT- Services

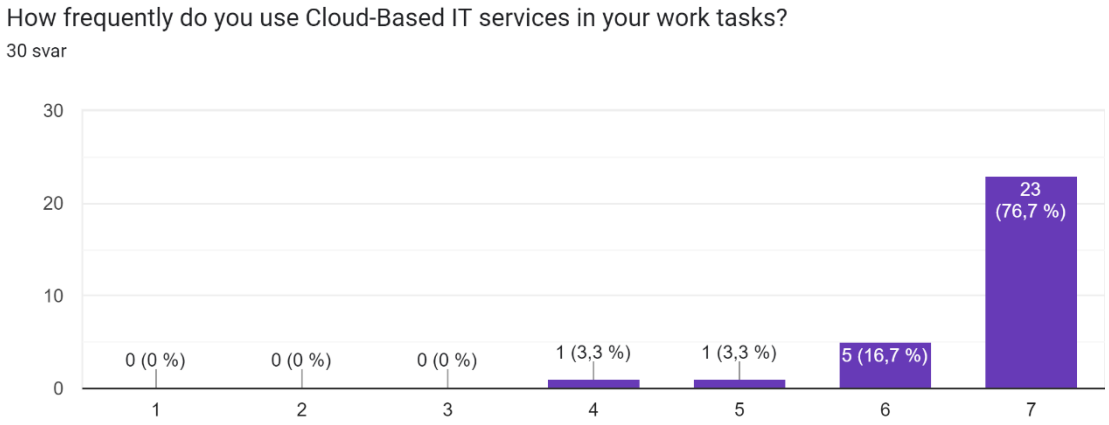

Figure 7: Results survey question 4: “How frequently do you use Cloud-Based IT services in your work tasks?”

Figure 7 depicts data that nearly all the respondents use Cloud-Based IT services to perform their work tasks. This question was designed to assess the participants' suitability for the study in addition to earlier methods of collecting participants. Furthermore, these questions set up the following questions to be asked. The question had to options to answer from 1-7. Where 1 was “Not very frequently”, the number 4 was “Neutral”, and number 7 was “Very frequently”. A majority 76,7% answered a 7, 16,7 % of respondents gave a 6, 3,3% of respondent gave a 5. One respondent stayed neutral choosing 4, which accounted for 3,3 %.

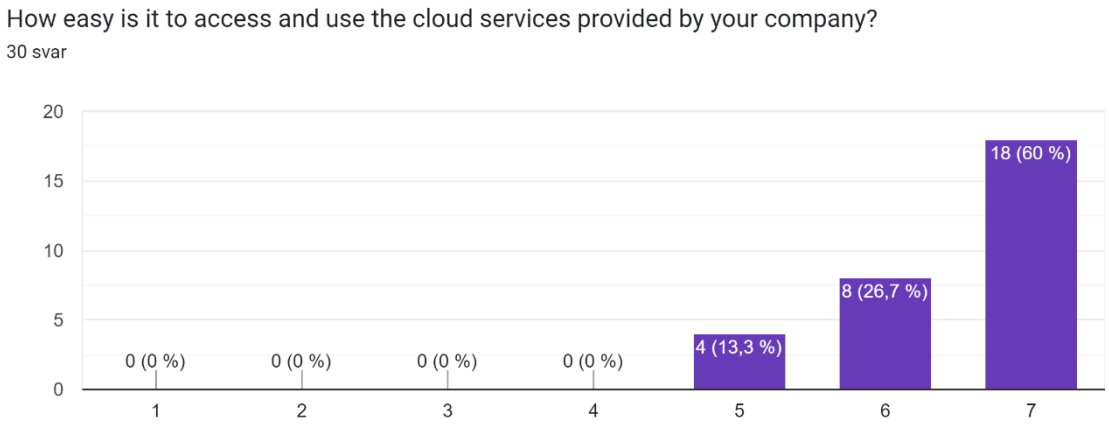

Figure 8: Results survey question 5: “How easy is it to access and use the cloud services provided by your company?”

All the respondents had a positive view, stating that it is easy to access and use their company's cloud services. The options were for this question was 1 for “Not very easy”, the number 4 for “Neutral”, and number 7 for “Very easy”. 60 % of the respondents selected 7, 26,7 % selected 6 and 13,3 % gave a 5.

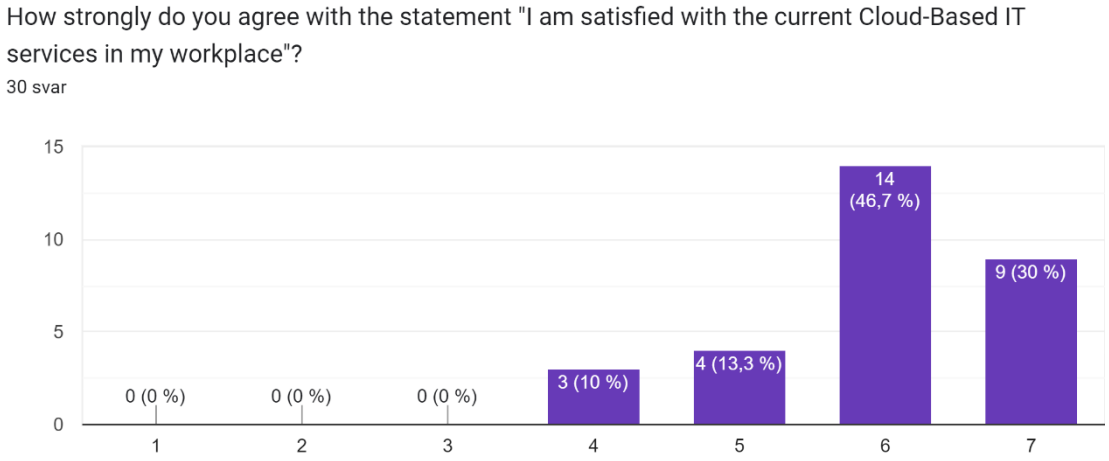

Figure 9: Results survey question 6: “How strongly do you agree with the statement “I am satisfied with the current Cloud-Based IT services in my workplace”?”

The data in Figure 9 indicates a generally positive view of the satisfaction with current Cloud-Based IT services in the workplace. This question was designed as a statement with the level of agreement from 1-7. Number 1 was “Not very strongly” 4 was neutral and 7 was “Very strongly”. For this figure 30% answered 7, 46,7% selected 6 and

13,3% gave a 5. The remaining 10 % were neutral and selected 4. The answers are somewhat split, which may indicate some concerns regarding satisfaction, but overall, the results are similar.

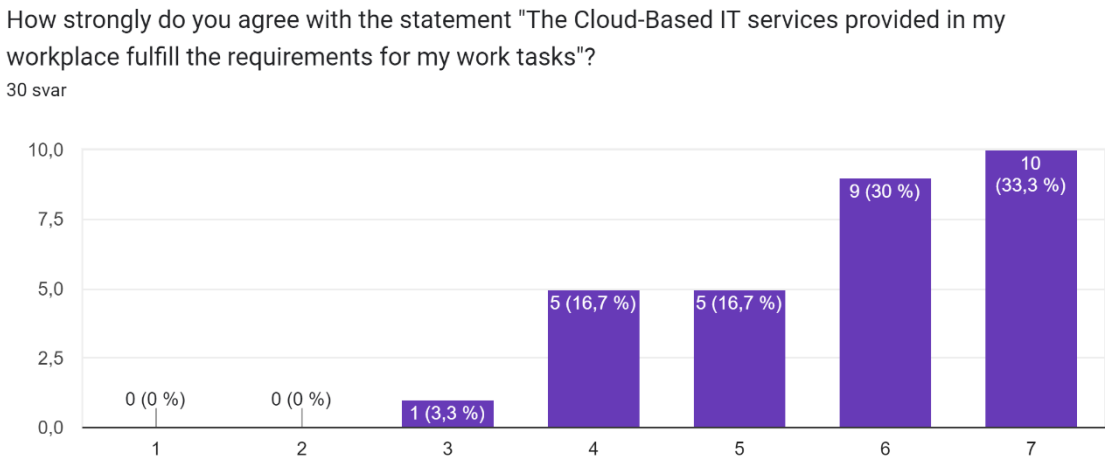

Figure 10: Results survey question 7: “How strongly do you agree with the statement "The Cloud-Based IT services provided in my workplace fulfil the requirements for my work tasks"?”

Figure 10 shows mixed results, but a large majority of the respondents are of the opinion that the services fulfil the work requirements for their tasks. The layout of this question was done similarly to the previous one. In the figure, 33% answered 7, 30% gave a 6, 16,7% selected 5. The amount of people answering 3 or neutral were 16,7%. Finally, 3,3% answered 3.

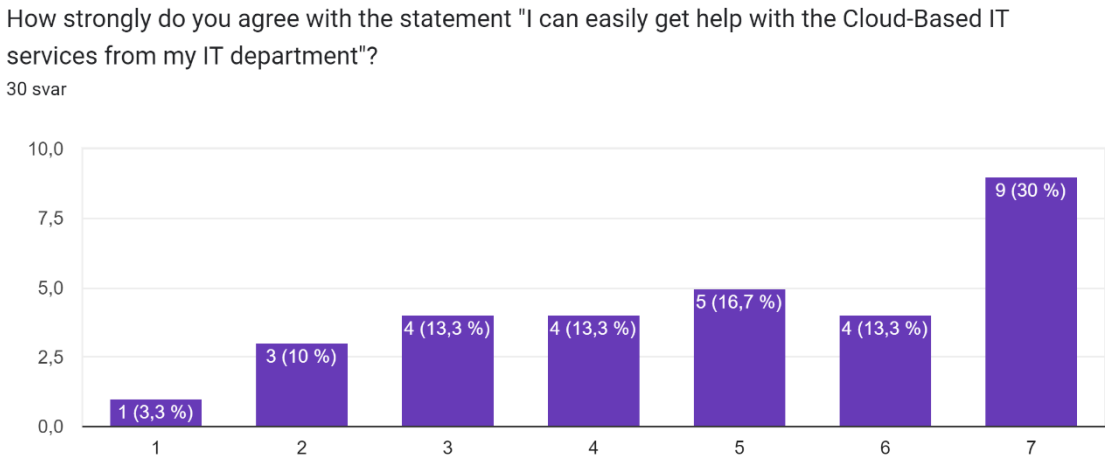

Figure 11: Results survey question 8: “”How strongly do you agree with the statement "I can easily get help with the Cloud-Based IT services from my IT department"?”

This question was used to indicate any dissatisfaction with the help provided by the IT department regarding the services. Before this question, the overall view of the respondents was more positive or neutral. However, in Figure 11, the answers start to show a more negative view. Still, most respondents remain on the positive side. On the positive side from 5-7, 30% gave a 7, 13,3% answered 6 and 16,7% selected 5. The respondents that were neutral or 4 were 13,3%. On the negative side 13,3% choose 3, 10% gave 2 and finally 3,3% answered 1.

4.3 Part 3: Questions about Cloud-Based Shadow IT

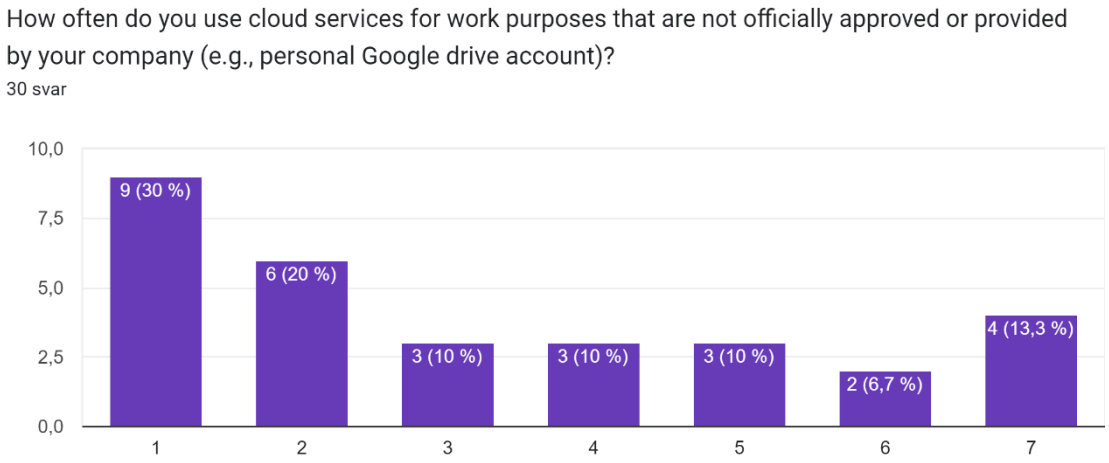

Figure 12: Results survey question 9: “How often do you use cloud services for work purposes that are not officially approved or provided by your company (e.g., personal Google drive account)?”

Figure 12 shows mixed responses as well. This question was used to assess the usage of non-approved cloud services in the workplace. Most respondents did not use non-approved services often. However, a notable 40% did use non-approved cloud services in their work to varying degrees. The ranges in this question were from 1 being “Not very often, 4 for “Neutral and 7 for “Very often. Here the positive side had 13,3% giving a 7, 6,7% a 6 and 10% selecting 5. 10% remained neutral. The negative side had 10% for 3, 20% for 2 and 30% for 1.

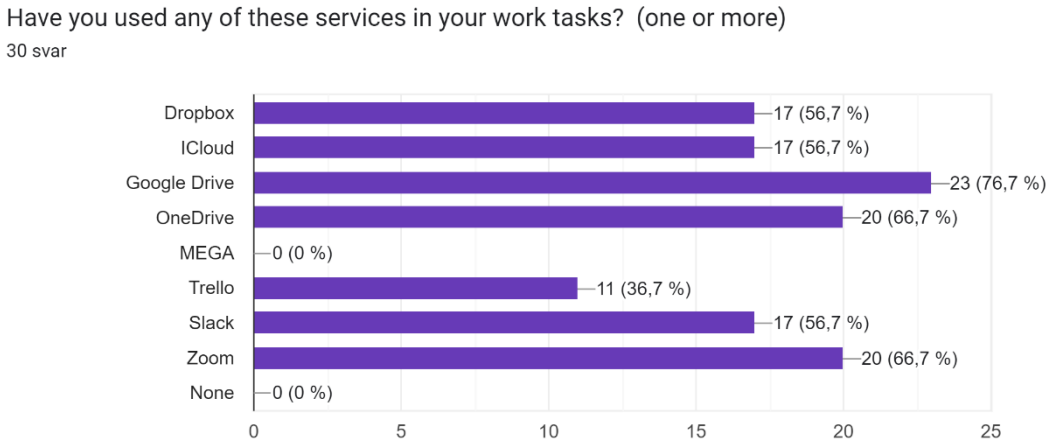

Figure 13: Results survey question 10: “Have you used any of these services in your work tasks? (one or more)”

This question mentions examples of services that are shown in the literature to be CBSIT. While these services are notable in the literature, they do not necessarily have to be non-approved by the IT department. Some of the services can be approved for usage in work tasks in their respective companies. The data shows that answers are split among the services, but they are being used, except for MEGA, which no respondent used.

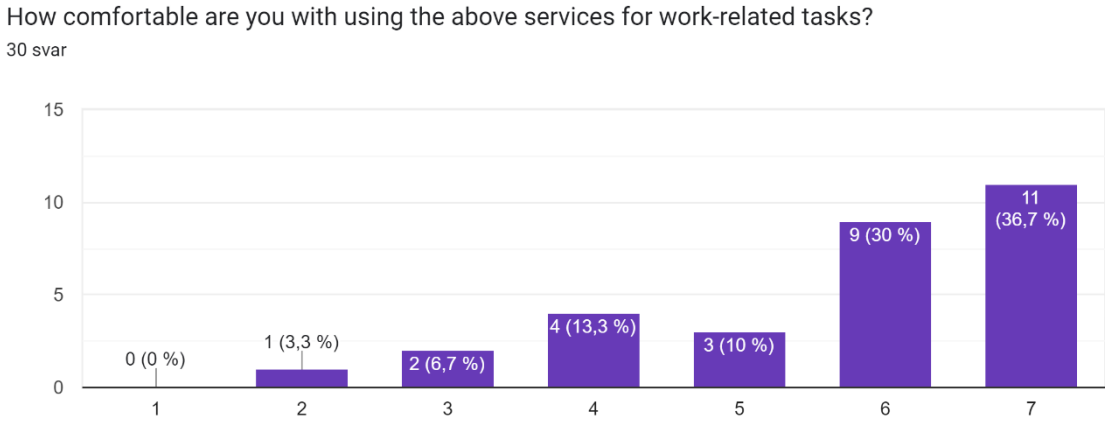

Figure 14: Results survey question 11: “How comfortable are you with using the above services for work-related tasks?”

Figure 14 indicates the comfortability of using these services from 1-7 with 1 being “Not very comfortable”, 4 being “Neutral” and 7 for “Very comfortable”. The results show 76.7% being comfortable to some degree with using the services for their work. 36,7% selected a 7, 30% gave a 6 and 10% a 5. 13.3% remained neutral in their response, and only 10% did not feel comfortable to some degree with these services. With 6,7% answered a 3 and 3,3% for 2.

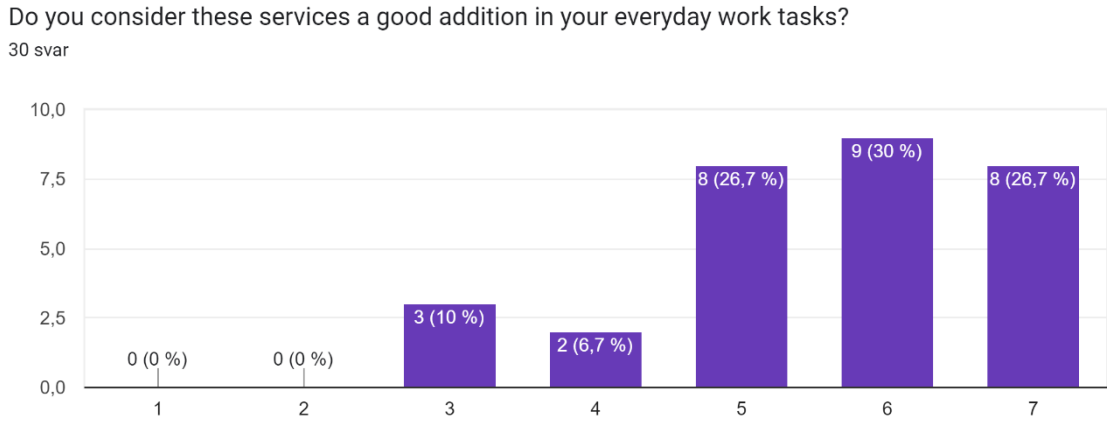

Figure 15: Results survey question 12: “Do you consider these services a good addition in your everyday work tasks?”

A follow-up question asked how these services help in their tasks. From 1 being “Not very good”, 4 for “Neutral” and 7 equalling “Very good”. The data shows a positive response, with 83.4% considering the services to be a good addition to different degrees. The figure shows 26,7% selected a 7, 30% a 6 and 26,7% a 5. 6.7% remained neutral, and 10% did not feel they were a good addition to a somewhat negative degree.

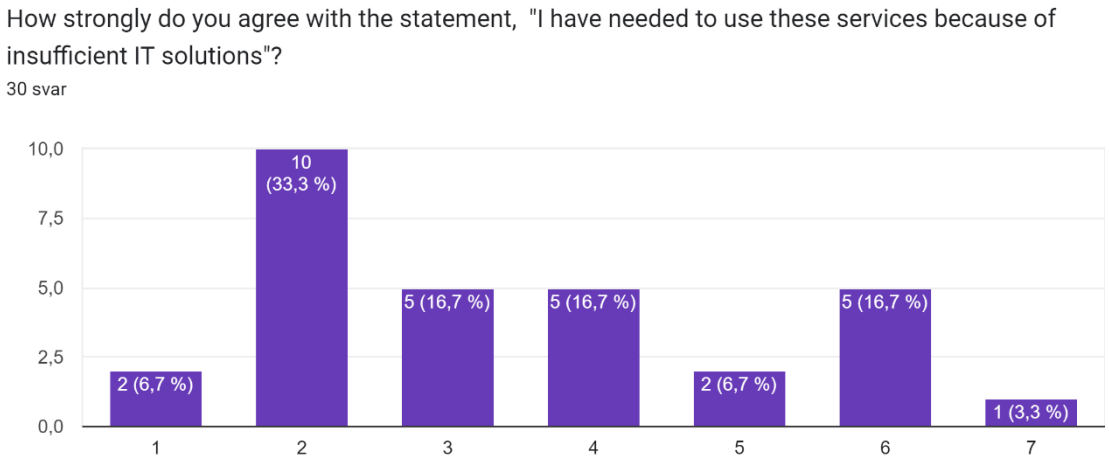

Figure 16: Results survey question 13: “How strongly do you agree with the statement, "I have needed to use these services because of insufficient IT solutions"?”

This question was designed to determine if these services are used in situations where regular options do not provide the necessary means to perform work tasks. Similarly to earlier statements the question ranged from 1 (Not very strongly), 4 (Neutral) and 7 (Very strongly). While some respondents felt that the services were a good addition to their tasks. 3,3% for 7, 16,7% answered 6 and 6,7% a 5. 56% of respondents do not feel that it is necessary to use them because of insufficient IT solutions. With 16,7% staying neutral.

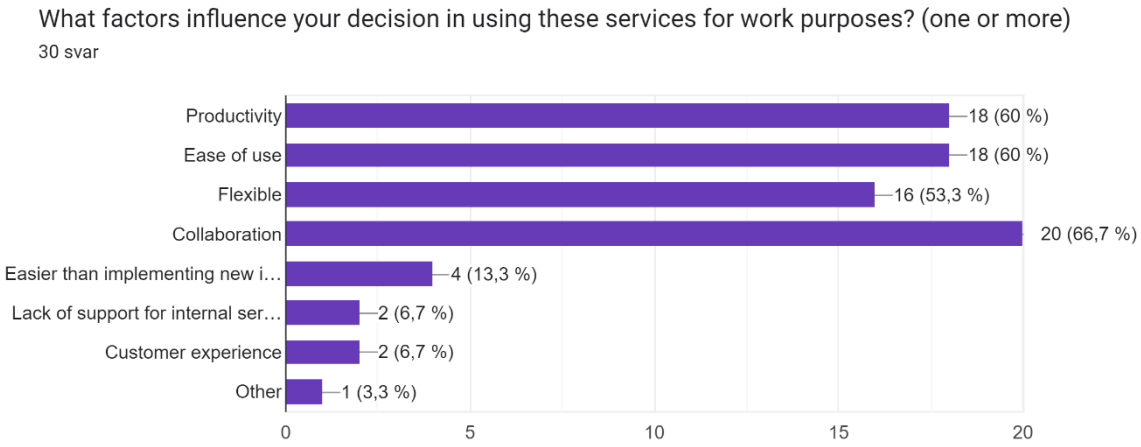

Figure 17: Results survey question 14: “What factors influence your decision in using these services for work purposes? (one or more)”

The potential options in Figure 17 were based upon key factors mentioned in the literature about Shadow IT and CBSIT. Most respondents chose the provided options, with "productivity," "ease of use," "flexibility," and "collaboration" being the most common factors.

Figure 18: Results survey question 15: “If other option, please state the reason”.

Figure 18 presents the answers from the other options in Figure 14. This option was included to allow respondents to provide individual answers that do not fit the above factors.

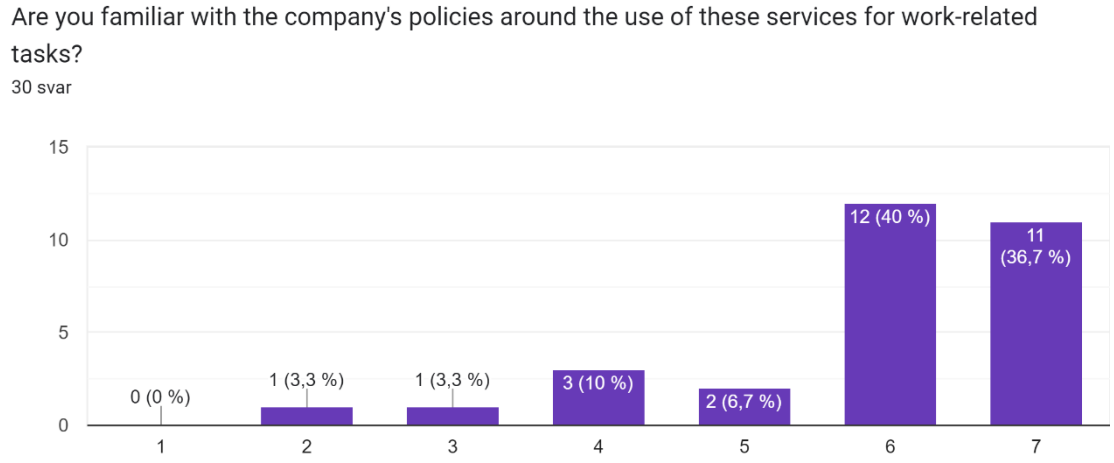

Figure 19: Results survey question 16: “Are you familiar with the company's policies around the use of these services for work-related tasks?”

The next question aimed to assess the employees' familiarity with their company's policies regarding CBSIT services. Ranging from 1-7 where 1 (Not very familiar), 4 (Neutral) and 7(Very familiar). A majority, 83.7%, were aware to some degree of the

policies. 36,7% answered a 7, 40% a 6 and 6,7% a 5. 10% gave neutral while 3,3% a 3 and 3,3% a 1.

4.4 Part 4: Cloud-Based Shadow IT

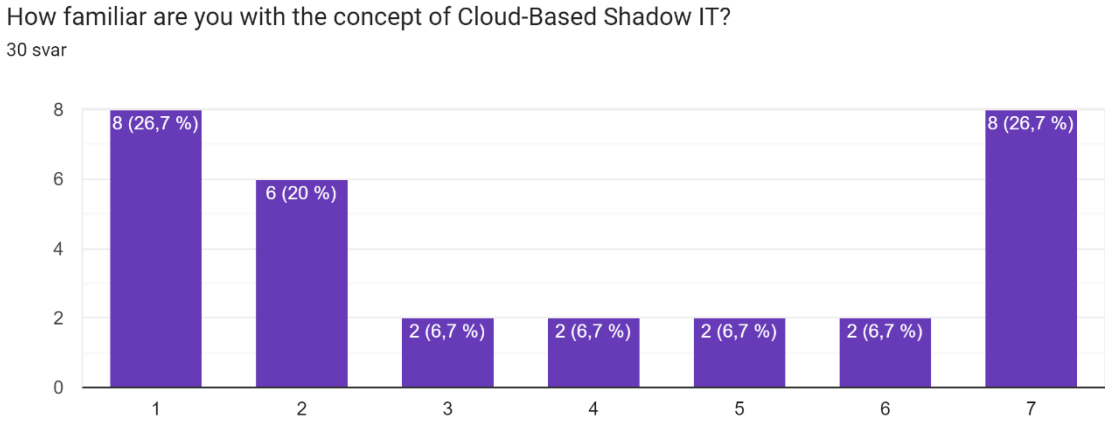

Figure 20: Results survey question 17: “How familiar are you with the concept of Cloud-Based Shadow IT?”

The data in Figure 20 reveals mixed answers regarding the respondents' familiarity with CBSIT. The similar ranges were adopted in this figure from the previous question. A majority, 53.4%, were not very familiar, 6,7% selecting 1, 20% a 2 and 26,7 answered a 1. While 40.1% were familiar, 26,7% gave a 7, 6,7% a 6 and 6,7 a 5. Moreover, 6.7% remained neutral in their response.

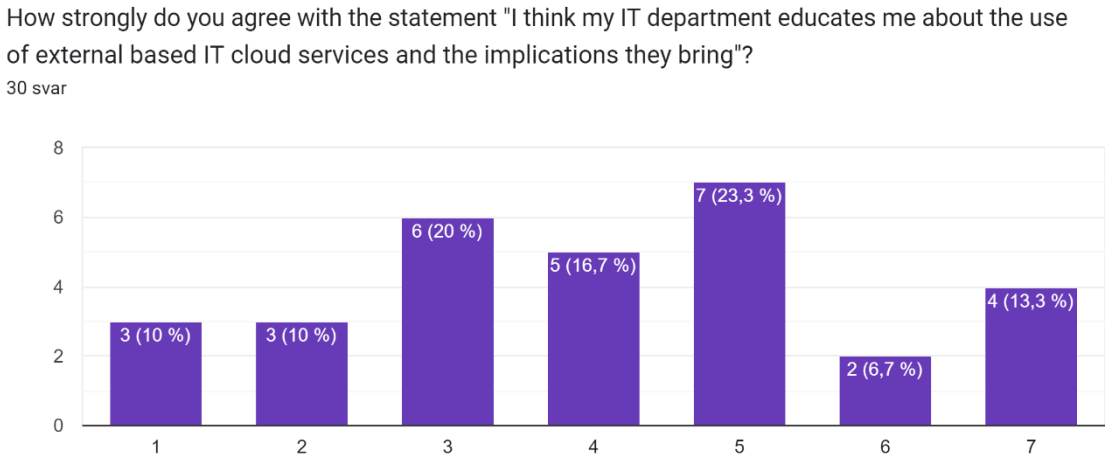

Figure 21: Results survey question 18: “How strongly do you agree with the statement "I think my IT department educates me about the use of external based IT cloud services and the implications they bring"?”

Results in Figure 21 gave similar ranges to earlier statements. It showed a mixed response, with most respondents leaning toward the middle, indicating that they feel somewhat educated or not about CBSIT from their IT department. 13,3% selected a 7, 6,7% a 6 and 23,3% a 5. 16,7% choose to be neutral. 20% answered a 3, 10% a 2 and similarly 10% a 1.

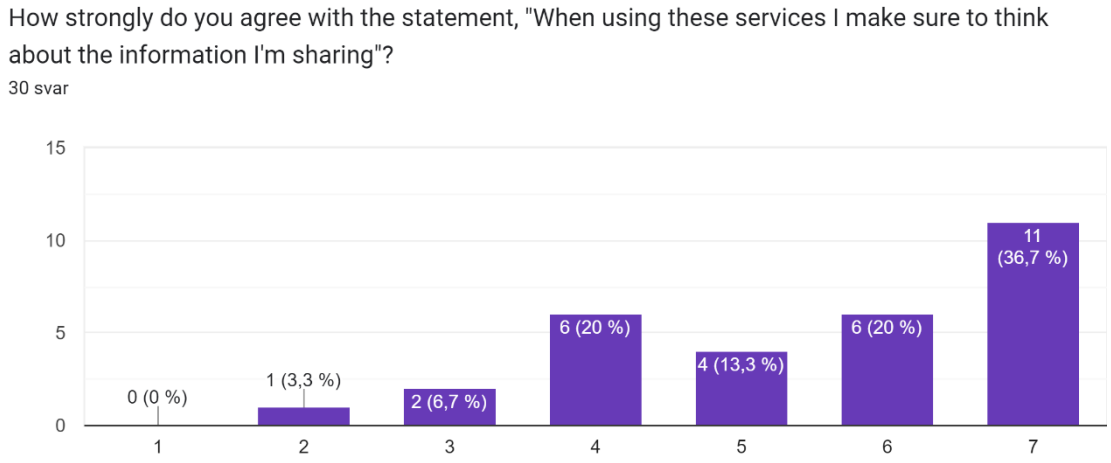

Figure 22: Results survey question 19: “How strongly do you agree with the statement, "When using these services, I make sure to think about the information I'm sharing"?”

Figure 22 employs the statement ranges from 1-7. It reveals that most participants, 60%, think about the information they are sharing to some degree when using these services. 36,7 % of respondents gave a 7, 20 % answered a 6, 13,3% a 5. 20% choose to be neutral. While 6,7% answered a 3 and 3,3% a 2.

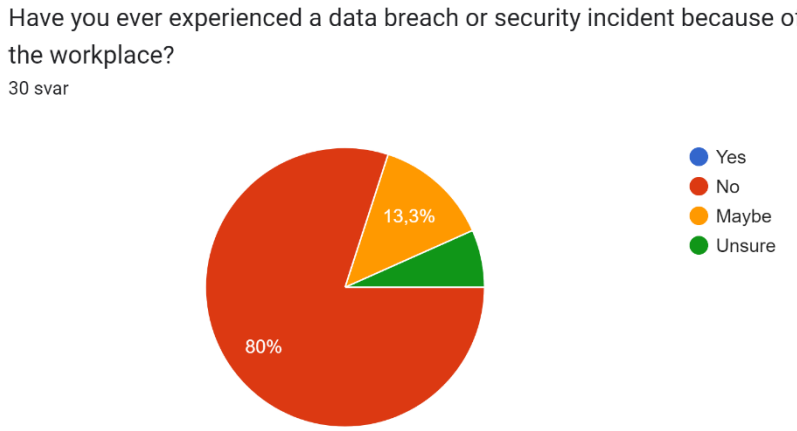

Figure 23: Results survey question 20: “Have you ever experienced a data breach or security incident because of any of these services in the workplace?”

In Figure 23, no participant knew if there had been a data breach resulting from using these services in their company. 80% answered "no," 13.3% answered "maybe," and 6.7% were “unsure”.

5. Results from Qualitative Study

The following section presents the results of a qualitative study conducted through semi-structured interviews with four individuals. It begins with an introduction of the participants and then delves into the themes that emerged from the interviews. The themes were selected upon reoccurring patterns from the interviews named accordingly.

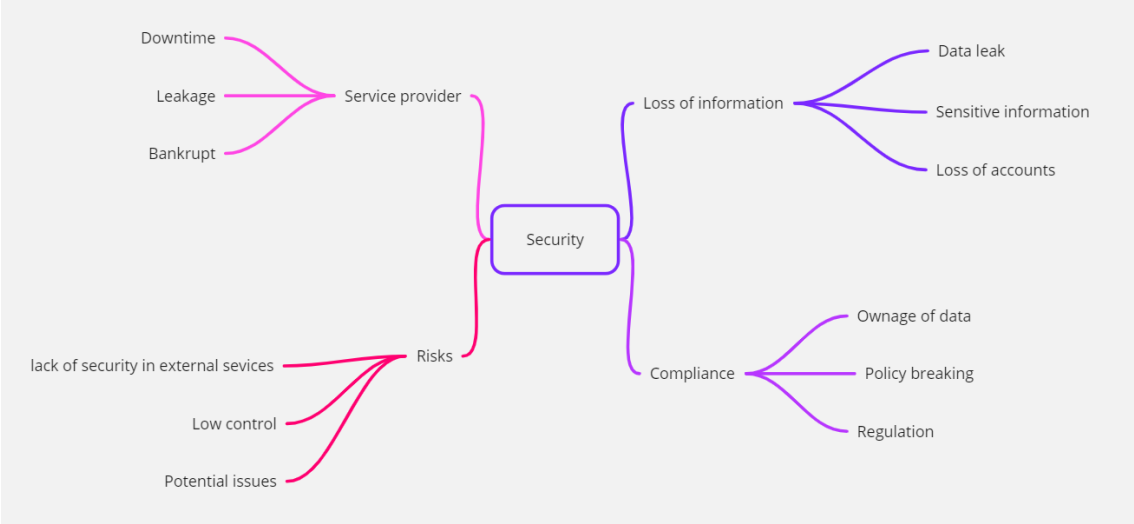

Figure 24: Example of coding for Security category

Security	Policies	Usage of cloud services	Education	Flexibility	Convenience	GDPR
Loss of information Risks Service provider Compliande	Awareness Compliance Monotoring Certifications Understanding	Collaboration Requirments Reliance Standardize service Islands of information Communication	Knowledge Requirments Protocols Training Migitate risk Onboarding Reading policies Adherance to policies	Changeable Nature of cloud services easy communicatioon Facilate communication Collaberation Easy as possible	Easy to set up Minimal effort Essential Minimize project time Appropriate solutions Adapting	Being informed Compliance Blacklist Personal data Implications

Figure 25: Identified themes and example of coding for categories

Figure 24 and 25 shows the process from coding to identifying the themes presented from the transcript. Figure 24 shows an example of the coding for the identified Security theme, where different codes that the respondents mentioned are looked upon to find the underlying theme that is discussed. Figure 25 shows all the identified themes that are categorised in the results, where there are examples of some of the codes that were looked upon for each theme.

5.1 Participant Profiles

Respondent 1: An IT consultant manager with four years of experience in a tech consulting firm and a total of 14 years in the field. Possesses a strong technical background and has served as a project manager on various sites in Sweden.

Respondent 2: Manages a development team in a company that specializes in safety solutions for different organizations. Has 16 years of experience in the field with a technical background. Responsible for managing workers across different sites in Sweden and maintains regular communication with them.

Respondent 3: Chief Product Officer with managerial responsibilities. Previously worked as a developer for eight years. Involved in the development of new platforms and internal systems for the organization.

Respondent 4: Commercial manager in a tech company with 6 years' experience that provides telecom solutions and services to international clients.

5.2 Security

Security emerged as a common concern among the participants. All respondents mentioned that security is a primary issue when using CBSIT or outsourcing cloud services to other companies. Two respondents also highlighted compliance issues as a risk for their organizations. Respondent 1 expressed:

> *"Yes, but the security question is probably the biggest and it encompasses a lot of different things. It's both about ownership of the data - do organizations or individuals still own the data or information that is transferred to another type of service?" – Respondent 1*

Respondent 2 held the opinion that data security is also a primary factor when using the services. However, they emphasized the consequences of breaking company policies and GDPR regulations. The respondent expressed confidence that the company did not have any security issues. They mentioned that relying on external services always

carries the risk of service downtime or the service provider going bankrupt, which could result in data loss and inability to restore it. The respondent highlighted the problem of losing all the information, including accounts and other related data, stored in such services. The company has established plans to address these types of scenarios and considers them important steps in dealing with potential issues. Respondent 2 acknowledged the inherent risks in using such services but compared it to the risk of using emails for sending files. However, they identified the biggest risk as potential data leaks and compromised organizational information.

> *"To go and attest it clearly or ask for permission. For example, I want to use service number x instead of working on it myself. If you want to take it further, you should use single sign-on for all and have a clear user-friendly structure in it." – Respondent 3*

Respondent 3 recognized the value of external services in the workplace but noted the lack of security aspects. They suggested implementing single sign-on as a solution to enhance control over these services, although they also acknowledged the associated cost implications. Respondent 3 pointed out that the absence of proper regulation leads to fragmented information across different departments, which further compromises security.

> *"One problem I can see for the CTO is that he always must be concerned about the security aspect. We are so spread out that information is available in many places, and I assume there may be security vulnerabilities. But I can't say exactly what is being done to address them. However, I would say this is the biggest issue. "– Respondent 4*

Respondent 4 identified security concerns as a significant challenge for the Chief Technology Officer (CTO). With information scattered across various services, the respondent emphasized the need for heightened security measures. However, they acknowledged a lack of knowledge regarding the specific security measures in place.

5.3 Policies

"We have pretty strict IT policies internally. Another question is how many people read them and are updated on them." – Respondent 1

Respondent 1 indicated that the company has strict policies regarding the use of approved services but questioned the level of awareness and compliance among employees. Although if employees follow the policies, the respondent highlighted the need for monitoring. Additionally, the respondent mentioned that many clients use alternative external services. In such cases, the company conducts a thorough analysis before collaborating, recommending services like OneDrive and Microsoft 365 due to their strong privacy foundation and established connections.

Respondent 2 shared a similar perspective, noting the existence of strict internal policies regarding the use of CBSIT. They expressed confidence that employees adhere to these policies, further reinforced by recent certification obtained by the company.

Respondent 3 acknowledged less stringent policies in place and identified a problem arising from employees' lack of awareness and understanding. The respondent mentioned that upcoming certifications would lead to a review of certain policies.

5.4 Usage of cloud services

"Most customers use cloud services, such as OneDrive or M365, but some use Dropbox or Google Drive. We ask why they use a particular service and if it meets their needs. We also ask about security, where their servers are located, and which sector they operate in." – Respondent 1

Respondent 1 feels that this is a particular topic in their organization as they sell the use of OneDrive to companies. They often question clients who use other services than theirs and why they rely on them. Saying they already have experience with the services and rely on them because of already created accounts and not much knowledge about the risks. Respondent 2 thinks they do have clear requirements for the cloud services they do take in and what is needed for their work tasks, where a group leader oversees budgeting and purchasing. Respondent 2 mentions as well that cloud services are addictive for companies; you rely most of the time on them to perform tasks, therefore it

can be problematic if an organization becomes too dependent on them. Having a service go down can affect collaboration. Using Teams, Slack, or Google Drive and experiencing an outage is a negative aspect.

> *"One advantage and disadvantage of cloud services is that it is easy to rearrange, easy to use and leave it. It can become very small islands of information, and eventually, there may not be a standardized solution for the company." – Respondent 3*

Respondent 3 feels positive about the usage of cloud services, both internal and external ones, but feels that the lack of standardized service has both positive and negative aspects. Referring that while employers feel that external cloud services are easy to set up by just creating an account and being convenient, it creates a whole lot of different solutions in the company where different teams are using different services and are unable to communicate with one another. Continuing to state that from a management perspective, it would be better to rely on one standardized solution from the company, where everything is agreed upon, and it would also benefit IT security standards.

> *"I work from home a lot, so we rely entirely on cloud services to work. We have discussed the services quite a bit, and many people have different opinions about them. Some people prefer one service, while others prefer another." – Respondent 4*

5.5 Education

The respondents highlighted the knowledge factor as a primary consideration in dealing with CBSIT.

> *"I think the most important thing is the security aspect and education is really important. It's about becoming aware of the choices you make." – Anna*

Respondent 1 emphasizes the importance of knowledge for workers to understand why a service is being used. In their company, they frequently ask and analyse client needs

to determine if the service meets their requirements. They acknowledge that this is more of an issue with clients, but internally, they have established protocols and systems to gather feedback.

Respondent 2 recognizes the risks of inadequate training in using these services, as it may lead to problems with GDPR and compliance with policies. However, they see no problem in their company, stating that the understanding of potential risks is higher due to the nature of working in a SaaS company. They also mention that they provide extensive internal training to mitigate these risks. Training for workers should be an ongoing process during onboarding, including reading and accepting policies.

> *"But learning how to upload a document to Teams or Dropbox may not come naturally. Because email is email, but a Teams chat is a Teams chat. It's just between you and us. It means you have to start diving deeper into technology." – Respondent 3*

Respondent 3 emphasizes the importance of education for employees in minimizing and adhering to policies when working with CBSIT. They note that removing it completely is difficult, and employers should avoid blaming workers. Instead, continuing education for employees is crucial so that they always keep it in mind while performing their tasks.

> *"We don't really have a process or conduct extensive studies on this. We've just picked things up along the way and seen what works and what doesn't. It's quite an informal way of doing things, but it works for us." – Respondent 4*

5.6 Flexibility

> *"We have a better culture internally in the company to be changeable and flexible and understand that things happen very quickly, and you have to keep up, and with customers it's a bit more sluggish or requires more decisions or hierarchy." – Respondent 1*

Respondent 1 recognizes the need for flexibility among workers to ensure that the services being used align with their needs and prevent them from relying on alternative solutions.

> *"One advantage and disadvantage of cloud services is that it is easy to rearrange, easy to use and leave it." – Respondent 3*

Respondent 3 acknowledges the flexible nature of cloud services and their ease of adoption within a company. However, they also mention that this flexibility can lead to unnecessary options within the company. They suggest a more standardized service that can facilitate communication across different teams, rather than relying on numerous different services. According to Respondent 3, centralizing the solution and clearly stating the cloud services in use would be a viable solution.

> *"My advice is that one must be pragmatic, and that basic security must be maintained, but then one must also be flexible enough to easily communicate with customers, partners, etc. It's always a give and take." – Respondent 4*

5.7 Convenience

Respondent 1 believes that convenience is an important aspect of why employers rely on Cloud-Based IT services. It is easy to set up and requires minimal effort, and she notes that the products use sales techniques to emphasize this factor. Furthermore, she mentions that group thinking can also play a role; if several people are using it, then it is not a problem for her to use it.

> *"It is far from reality today to not use cloud services." – Respondent 2*

Respondent 2 focuses on the fact that cloud services are now essential for companies to perform their work effectively. They highlight that these services are easy to use and set up.

Respondent 3 recognizes the clear convenience of using external cloud services and the resulting reduction in administrative and project time. They also note how these services enhance workers' effectiveness and provide clear benefits to the organization through ease of use and improved communication.

> *"We use Slack and similar tools extensively, as they are the standard means of communication for us." – Respondent 4*

Respondent 4 notes that their company does not have a formal process in place for using these cloud services, unlike other companies. Instead, they rely on their own experiences and pick up the most appropriate solutions along the way. They emphasize the importance of making the use of these services as easy as possible, especially when collaborating with clients. They state that they do not want to impose a specific solution on clients but instead adapt to their preferences.

5.8 GDPR

> *"You need to be aware of privacy issues or ownership issues or other factors that may affect your choice. It's about becoming more informed and understanding that it actually affects things where goods lie in things." – Respondent 1*

> *“It's important to know where the data is, especially with GDPR in mind. It's also important that the services can deliver and solve the necessary problems.” – Respondent 2*

Respondent 2 emphasizes the importance of ensuring GDPR compliance when purchasing products and being aware of where the data is stored. They also highlight the need for the services to address and resolve any necessary issues. Respondent 2 mentions that in their company, employees do not use other types of services as there are procedures in place to protect data and policies that must be followed. However, they state that the provider they use is appreciated in the workplace, which may contribute to their choice. They further state that they do not have a procedure to

blacklist any programs used for communication with clients through external cloud software or third-party vendors.

> *"I should not send an unencrypted Excel sheet over email. No, you shouldn't, because GDPR has taught us that." – Respondent 3*

Respondent 3 acknowledges that while employees understand the GDPR implications of using personal information over email, they may not be as aware when it comes to using cloud services. They mention having processes in place to blacklist Excel files sent via email, but not through cloud services.

> *"Sometimes the administrators can be within our company, and sometimes they can be another company. But I am a little uncertain about what GDPR complications this may have." – Respondent 4*

Respondent 4 expresses uncertainty regarding the GDPR implications of having administrators from either their own company or another company. They mention having made changes when GDPR came into effect, such as revaluating their monthly email lists to clients. However, they are unsure about GDPR implications for similar usage with cloud services where personal data might be present.

6. Quantitative Data Analysis

The following text presents the analysis of the quantitative data from the survey. The data is from 30 participants from the tech sector. Part 1 presents and analyses the demographic information. Part 2 includes data about the use of cloud services and policy awareness. Part 3 notes specific usage of cloud services, and Part 4 looks at awareness of CBSIT and security.

6.1 Part 1

Gender

Gender	Frequency	Percentage
Male	24	80%
Female	6	20%

Table 4: Survey question 1

Gender imbalance: The respondents were primarily male, which is not too surprising, given that the majority are males in the tech sector. In the tech sector generally 75% are male and 25% are female (Swift et al, 2015). Having gender as a demographic was brought up to look at if the gender of the respondents were in accordance with the general gender of the population of the tech sector.

Age Group

Age Group	Frequency	Percentage
Gen Z (18-26)	1	3,3%
Millennial (27-42)	10	26,7%
Gen X (43-58)	17	53,3%
Gen Jones (59-68)	3	13,3%
69 +	1	3,3

Table 5: Survey question 2

Age distribution: The top group was Gen X. Age is an interesting factor in survey studies, where it is reported that older individuals tend to be more open to answering surveys in comparison to younger generations (Gigliotti & Dietcsh, 2014). From the

results this assumption holds true to some degree, however the most respondents seem to be around the centre of age groups.

Experience

Years of Experience	Frequency	Percentage
0-2	3	10%
3-5	3	10%
5-9	2	6,7%
15+	22	73,3%

Table 6: Survey question 3

Experience level: Most participants were considered experienced in the tech sector. The experience demographic was brought up on the assumption that the more years of experience the respondents had the more they would be aware of the questions. In addition, they could have answered differently. However, no answers were significant enough that would support this.

6.2 Part 2

Question	Sum	Mean	Median	Mode	Standard Deviation	Confidence Interval 95%
How frequently do you use Cloud-Based IT services in your work tasks?	200	6.63	7	7	0.71	(6.37, 6,83),
How easy is it to access and use the cloud services provided by	194	6.43	7	7	0,73	(6.16, 6.69)

your company?						
How strongly do you agree with the statement "I am satisfied with the current Cloud-Based IT services in my workplace"?	179	5.96	6	7	0.93	(5.62, 6.29)
How strongly do you agree with the statement "The Cloud-Based IT services provided in my workplace fulfill the requirements for my work tasks"?	172	5.73	6		1.2	(5.21, 6.24)
How strongly do you agree with the statement "I can easily get help with the Cloud-Based IT services	147	4.9	5	7	1.88	(4.22, 5.57)

from my IT department"?						

Table 7: Survey question 4-9

Two analyses were performed on the Crohn's alpha on the questions above, the first were through questions 1 to 4 and later questions 1 to 5. The first noted a correlation efficient of 0,75 equalling an acceptable consistency between the questions. In the second measurement a correlation efficient of 0,64 was noted which equals a lower level of inconsistency when the last question was introduced (Crobach's 1951). Indicating a moderate internal consistency.

The analysis shows that respondents favour the use of cloud-based services in the workplace and find them easy to use. There are some concerns regarding the requirements and satisfaction of the services. It is also noted that there are mixed feelings about the ease of support from the IT department regarding the services. However, most respondents still answered favourably. Huleboschh (2016) writes about this in their paper on how employees can avoid contacting the IT department due to lengthy processes. Jones et al. (2004) also write about this perspective, where employees trust the solutions of the IT department but may turn to other solutions when the contact process is lengthy.

6.3 Part 3

Question	Sum	Mean	Median	Mode	Standard Deviation	Confidence Interval 95%
How often do you use cloud services for work purposes that are not officially approved or provided by	97	3.23	2.5	1	2.17	(2.36, 4.09)

your company (e.g., personal Google drive account)?						

Table 8: Survey question 10

Have you used any of these services in your work tasks? (one or more)

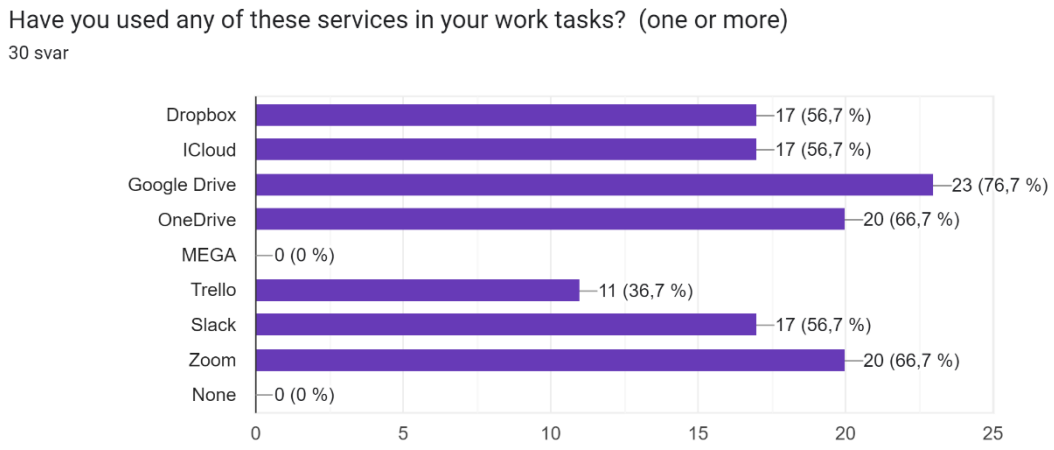

Figure 13: Results survey question 10: "Have you used any of these services in your work tasks? (one or more)"

Question 1 of part three indicates that while some of the respondents do use cloud services that are not approved, the majority do not use them very often.

While the respondents in question 1 noted that most of them did not use unapproved cloud services, the second question indicates that there might be respondents who use non-official services. However, it is important to recognize that the question does not ask if these services are approved or not. Still, it may give insight into the understanding of the respondents' usage. If we consider the study by Netskope (2021) that states that 97% of cloud services in enterprises are not approved by the IT department, there may be tendencies to consider that the respondents are not aware if the mentioned services are approved or not.

Question	Sum	Mean	Median	Mode	Standard Deviation	Confidence Interval 95%
How comfortable are you with using the above services for work-related tasks?	170	5.66	6	7	1.44	(4.85, 6.46)
Do you consider these services a good addition in your everyday work tasks?	167	5.56	6	7	1.25	(4.99, 6.12)
How strongly do you agree with the statement, "I have needed to use these services because of insufficient IT solutions"?	104	3.46	3	2	1.71	(2.77, 4.14)

Table 7: Survey question 12-16

The data from the questions indicates that the respondents generally feel safe using the services, see them as a good addition to their everyday work tasks, and that some respondents have needed to use the services due to insufficient IT solutions. However, most of the respondents did not use the services because of insufficient IT solutions. So,

while the respondents felt that the IT solutions were adequate, there may be other factors that lead them to use these services. Müller et al (2015) notes that employees see the ease of use of the services and their ease of setup in an organization. Additionally, respondents generally felt that these services were a good addition to their tasks. This can indicate what Gomez et al (2022) explains, where the services are used because of the benefits they provide in terms of productivity and new ways to solve tasks. However, the official IT solutions may be adequate for performing the same type of tasks.

What factors influence your decision in using these services for work purposes? (one or more)

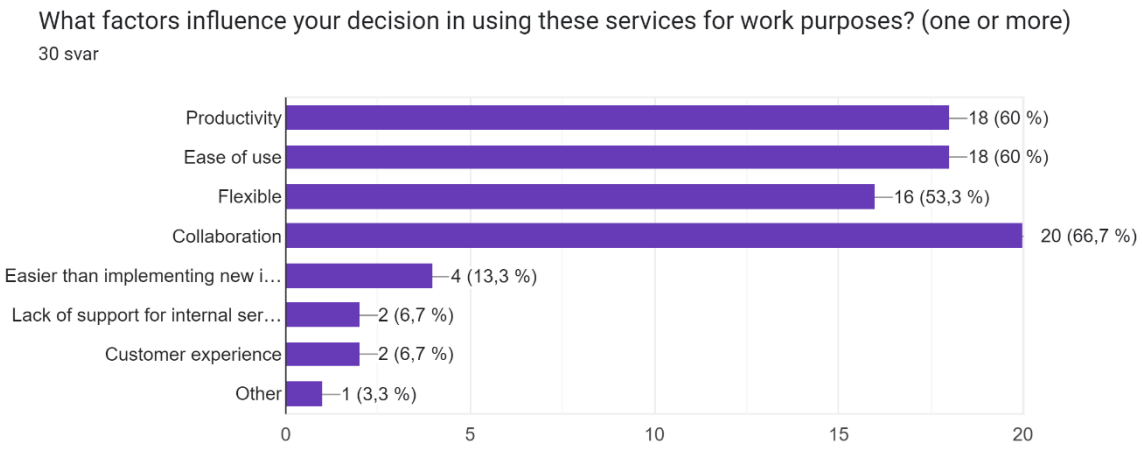

Figure 17: Results survey question 14: “What factors influence your decision in using these services for work purposes? (one or more)”

Figure 18: Results survey question 15: “If other option, please state the reason”.

The factors for this question above were chosen from the most common reasons for using CBSIT in literature. Most of the respondents seem to agree with the factors in place, which can indicate agreement with factors that the literature has already established.

Question	Sum	Mean	Median	Mode	Standard Deviation	Confidence Interval 95%
Are you familiar with the company's policies around the use of these services for work-related tasks?	176	5.86	6	7	1.30	(5.17, 6.54)

Table 9: Survey question 19

The respondents indicated good familiarity with the policies in place in the organization. Milne and Culnan (2004) state in their article that having good knowledge about the policies in place correlates with increased awareness of security risks and potential consequences of using external services in a company. However, if we consider the example by Nasuni (2012), where half of the participants in a survey of 1300 noted that they were aware of the policies in place but still used CBSIT in their work tasks, this can similarly indicate that the respondents are aware of the policies but still choose to use the services.

Crobach's Alpha Coefficient was calculated for the Likert scale questions in part 3, the coefficient was found to be 0.68. Which is just under the 0.7 of acceptable scale. This

indicates a moderate to almost good correlation (Crobach's 1951). The questions do however, vary in nature which can in turn affect the correlation between them.

6.4 Part 4

Question	Sum	Mean	Median	Mode	Standard Deviation	Confidence Interval 95%
How familiar are you with the concept of Cloud-Based Shadow IT?	112	3.73	3	1 and 7, Both occurs 6 times	2.47	(2.62, 4.83)
How strongly do you agree with the statement "I think my IT department educates me about the use of external based IT cloud services and the implications they bring"?	122	4.06	4	5	1.81	(3.45, 4.66)

How strongly do you agree with the statement, "When using these services, I make sure to think about the information I'm sharing"?	165	5.5	6	7	1.50	(4.85, 6.14)

Table 10: Survey question 20

The following questions above were used for calculation of the Crohn's alpha coefficient. The reported coefficient was 0.83 which is considered a good internal consistency. For the whole study Crohn's alpha coefficient was calculated from the questions with a Likert scale (1-7). For all the questions of Likert-scale the Coefficient was 0,66. This number is between the ranges from 0,7 which indicates acceptable for research and 0,6 which can indicate reason for revaluating the questions (Crobach's 1951). This can in hindsight be because some of the questions measure different concepts, one being the usage of regular cloud services and then moves on to CBSIT. However, 0,66 is not far from 0,7 and in this case, it can be argued that there is close to internal consistency for the whole study.

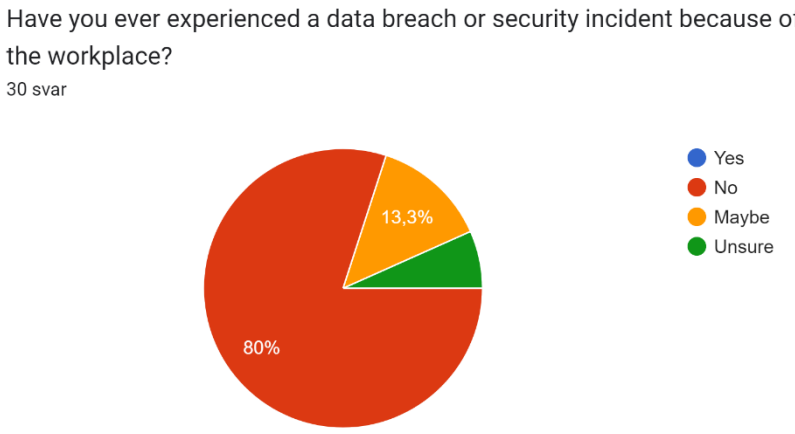

Figure 20: Results survey question 20: “Have you ever experienced a data breach or security incident because of any of these services in the workplace?”

Jonas et al (2004) suggest that the main reason for employees' usage of Shadow IT is the lack of current existing solutions that fit their work needs. In the survey, this was not clearly shown, but the underlying pattern of this existed. For example, in figure 20, the majority (56%) did not feel the need to rely on these services because of insufficient IT solutions. However, the usage of these services seems established and comfortable for the employees. All the participants had used the services mentioned, as noted in figure 10. However, the question does not ask if the services were already approved in the organization. Therefore, the results of the question are unable to fully conclude that they were indeed CBSIT. Still, the respondents in the question selected several of the services that were shown, this can indicate that some of the selected services are indeed not approved in the organization. As having licenses to several of the services for one IT-department can be unlikely. Puhakainen & Siponen (2010) note in their article the lack of awareness about Shadow IT and that users may not be aware that it is not allowed in their policies or that they have not received proper education about its use. Indications of this were shown in figure 11, where 76.7% of participants were comfortable with the usage of the mentioned services. Additionally, 83.7% in figure 16 stated that they knew to some degree about the policies regarding the usage of these services in the workplace. However, in figure 17, the majority (53.4%) did not know what CBSIT was, and a mixed response in figure 18 showed different opinions about how the IT department educated about these services: 40% did not feel that they did to

some degree, 16.7% were neutral, and 43.3% felt that their IT department did educate about the matter.

7. Qualitative Data Analysis

The following chapter will use the literature to analyse the results from the semi-structured interviews. A thematic analysis is performed where key components of the interviews are analysed and compared to the literature.

The identified themes for the semi-structure interviews are found below. The themes were found through the underlying categorization of what the respondents mentioned in the transcript and coded to find themes found in literature. The data from the respondents were then categorized and analysed under each heading. The elements of interest for the data were through an understanding of the literature and broken down to find patterns. Finally, the names of the themes were based on the subjects they touched or through underlying patterns in the transcripts.

7.1 Security

All the respondents identified security as a major issue of CBSIT, noting the risks of organizations sharing confidential information or exposing themselves to harmful activities. This aligns with the findings of Silic & Back (2014) in their study of IT managers, where the primary concern was that Shadow IT opens the internal network to malicious activity. Respondent 1 highlights the security aspects of data protection, questioning whether organizations still retain ownership of the data when it is transferred to another service. Intel (2017) touches on this subject, noting the negative effects of sharing data with third-party services on data compliance and emphasizing the organization's responsibility in ensuring compliance with legal requirements.

Respondent 2 raises concerns about data access and potential loss when using such services but does not delve into the subject of legal policies within their own organization. They express confidence that no one in their organization uses other services. Respondent 3 acknowledges the problem of creating islands of information by storing data in external services, making it challenging to ensure compliance with regulations. Respondent 4 also sees this as a concern for their company's CTO, who is consistently mindful of these risks when considering the use of such services. The respondents have different experiences but from their answers it does seem that the

security aspect is acknowledged as a concern from them. Which can tend to be a need for more increased awareness about security and need for proper procedures. Walter (2013) further discusses this issue in their paper, stating that organizations relying on storing data in external cloud services are not following the legal policies established for the organization. However, the author notes that there is a lack of strategies to address this. From the respondents there seems to be different opinions about this issue and indications of further research needed to address this. Similarly, to the literature the findings seem to indicate a need for proper procedures to address security concerns for CBSIT.

7.2 Policies

Three of the respondents believed that their own organizations had strict policies on CBSIT, but there were different opinions regarding the employees' awareness of these policies. Respondents 1 and 2 believed that employees in their organizations fully complied with the policies and understood them well. However, Respondent 1 noted a lack of robust policies among their clients regarding CBSIT. Respondent 3 indicated that the policies in their organization were not well-defined and lacked consistent enforcement. None of the respondents provided further details on why the policies were well understood. Respondent 1 mentioned the absence of studies within the organization but expressed confidence that the policies were being followed. Respondent 2 assumed compliance based on employee certification. Although Respondents 1 and 2 stated that they followed their IT policies effectively, it would be beneficial for the company to conduct further analysis on the matter. Seddon and Currie (2013) pointed out that cloud regulation is often not adequately addressed in IT policies. Furthermore, BT (2015) observed that while most IT security incorporates various potential IT risks, cloud services tend to be neglected. Although the respondent did not provide specific details about their organization's policies, maintaining the assumption of keeping their company's IT security private, it would be worthwhile for managers to explore ways to improve understanding of third-party software usage (Gozman & Willcocks 2019). In contrast to the literature the respondents felt mixed in their opinions about their policies, this which can indicate more reason to further study the specific policies in place.

Behrens (2009) found in their study that employees feel compelled to circumvent policies due to a lack of understanding or overly strict guidelines. Silvius and Dols (2012) further noted that employees' unfamiliarity with the policies in place resulted from inadequate training, rendering them unaware of the associated implications. Respondents 1 and 3 expressed concerns about employees' understanding of the policies. Respondent 1 focused more on their clients, stating that it is unclear whether the policies are followed within the organizations and that no system for follow-up is implemented. Akande, Akinlolu, and April (2013) addressed the lack of standardization in CBSIT, which can make policies difficult to follow and understand. György et al (2012) also bring up the importance of having governance over the user-driven innovations like Shadow IT to minimize the risks. From the literature and the respondents, it's seeming well-important to consider the policies in place and state organization can benefit from better policies on the usage of CBSIT. The communication of the policies on a regular basis could also make employees keep up with them when making decisions.

7.3 Usage of Cloud Services

The respondents' usage of cloud services revealed varying perspectives based on their own experiences. From the results, it is evident that most of the services mentioned in this report, such as OneDrive, M365, Dropbox, and Google Drive, were used. The respondents provided different answers regarding licensing. However, indications from the interviews suggested that in some cases, the services used were not properly licensed. Respondent 2, however, expressed confidence in ensuring the use of licensed services as the only service in their organization. Walters (2013) mentioned the issues associated with relying on these services to store company information, noting that such usage typically goes against organizational policies. A notable risk mentioned by the respondents is that the responsibility for data stored on these services still lies with the organization. If access to these accounts is lost, it poses a compliance issue (Lewis 2016). Having not properly used licensed can from the interviews seemingly lead to a harder time conducting analysis on the usage and the data that is on these services.

The results also indicated that organizations could become overly dependent on the use of cloud services in today's environment. Respondent 2 highlighted the role of

downtime in the workplace, which poses a risk to collaboration. Respondent 3 addressed the challenges arising from different cloud services, resulting in the creation of islands of information and hindering collaboration within departments. Respondent 3 also referred to what Jones et al. (2004) mentioned about Shadow IT, where the lack of communication and proper agreement between departments increases the use of unauthorized services outside the IT department's approval. Respondent 3 further stated that employees turn to such services due to their ease-of-use, low cost, and potential for increased productivity, acknowledging the diverse range of internal and external service options. Müller et al. (2014) explored this factor in their study, noting that these free alternatives are easier to set up compared to undergoing a lengthy approval process within the IT department. In reflection it is therefore not unthinkable that employees make the easier decision in turning to an ease-of-use alternative than conducting lengthy approval processes.

Respondents 1, 3, and 4 mentioned that different employees and departments have varying needs for cloud services, leading them to seek what works best for their respective tasks, ultimately enhancing productivity. Users may also feel inclined to choose services they are personally familiar with. Respondent 4 emphasized the importance of different services when working from home, adapting their usage to meet client needs. These factors align with the arguments presented by Haag and Eckhardt (2017), who contend that CBSIT compels employees to use services that best fit their needs. Calling it Personal IT which often bases on personal experiences with the programs in their personal lives which then apply to businesses.

Overall, the usage of cloud services within the organizations, as reported by the respondents, appears informal. They expressed positive views about cloud usage, with requirements varying across departments. However, there seems to be a lack of standardization, and no respondent could provide a clear answer on how to address this issue. This reinforces the idea from the literature that the phenomenon of CBSIT is often neglected within organizations, and greater recognition of the problem is necessary (Akande, Akinlolu, & April 2013). In addition, that user innovation solutions like CBSIT and governance of them can often be overlooked by management (Silic et al, 2016). IT departments can therefore have in increased reason to help management in guiding the governance of business units (Chua and Storey, 2016). In this case when

dealing with CBSIT as it seems there are similar problems to regular Shadow IT. The findings therefore align with literature that CBSIT seems neglected in analysis, focusing more on the positives of usage.

7.4 Education

All the respondents showed the importance of ensuring that education is vital for organizations to understand and adhere to policies. It is also important to understand the risks of CBSIT (Walters 2013). Respondent 1 felt that knowledge about the risks of the services helps create awareness in the organizations and how employers use the services. The education should be laid out so that employees can make decisions on their own when faced with issues that might conflict with policies. Furthermore, Respondent 1 notes that having knowledge about the issues helps when dealing with collaboration with business partners. Respondents 2 and 3 take the approach of continuous learning for employees to help them understand the policies put in place. Ali et al (2020) brings up the need for managers to help employees understand the reasons behind the adoption of a cloud service, as well as the reasons why the policies put in place for the services in use are there. Walters (2013) states the need for education to understand and shape the best practices. Having best practices can be thought to be of interest to many, there seems to be a need to incorporate and figure out what they are for CBSIT. The findings from the respondents are well withing what the literature states, that education of these issues are important to understand and be aware of the phenomenon.

7.5 Flexibility

Three of the respondents noted flexibility as a factor in internal and external cloud services. It allows for better collaboration for workers and better availability when telecommuting. Notably, it seems that the respondents feel that they want to be flexible with clients to meet their needs and collaborate with them. Respondent 1 notes that they themselves can depend on their flexibility with cloud services, but with clients, this is sometimes not the case, and they must adapt to their needs. Respondent 4 felt that they themselves were flexible for their clients to adjust their own services to what others are using and what clients feel works. They note that keeping tight regulations on the

services in use, in turn, hurts the flexible nature of cloud services. Cloud services being flexible has downsides, according to respondent 2 and 3. Respondent 3 mentions that it creates a lack of standardization in the organization because of the flexible nature, creating various services for employees to take advantage of. There seems to be indications that while flexibility is useful, there is need for organizations to find a way that best suits them. This can be an important view to discuss when bringing up Wafa'a & Khalid, 2020 who state the benefits of cloud services as being flexible and scalable.

7.6 Convenience

A notable theme from the respondents is the convenience that Cloud-Based IT services give to the workplace. Respondent 2 sees that cloud services, in general, are easy to set up while being low cost. Respondent 3 looks at the benefits in admin time and reduction in project times, while also making workers more effective at their tasks. Respondent 4 deems external cloud services essential to keep up with communication with clients. Cloud-Based IT services seems to be seen as beneficial for the daily tasks that the respondents face. It helps them work their tasks in a more efficient way and provides new solutions.

While Respondent 2 focuses on the more licensed cloud services in his opinions, he does imply that this is the general assumption of all cloud services and their motives behind their use. Similarly, Respondents 3 and 4 seem to understand why employees turn to it because of the convenience it offers. Gozman & Willcocks (2019) noticed in their study that turning to external cloud services allows employees to make use of a service without proper reliance on the IT department process and best practices. The authors also point out that employees who are pressured into following deadlines have a higher chance of avoiding these policies to finish their tasks.

7.7 GDPR

All the respondents mention GDPR in various ways and how it affects their organization since it came into effect. Respondent 1 focuses on the ownership of data on the platforms, noting that when dealing with the decision-making of the cloud services, GDPR must be considered, indicating the importance of organizations being aware if

they are GDPR-compliant. Respondent 2 also emphasizes the importance of knowing where the data is.

Respondent 3 brings up that GDPR has taught the company various new policies since it came into place, taking the example of not sending over an unencrypted Excel file. They have also taken measures to block these types of sharing through email. Respondent 4 mentions the new procedures in place when GDPR came into effect and how the organization adapted, but they were unaware of any new procedures regarding the use of cloud services. Both Respondent 3 and 4 noted that there were no such measures for personal data for the cloud services in the organization, although they have similar requirements as GDPR. This perspective indicates a potential gap in the protection policies for data in the organizations.

8. Discussion

The discussion chapter answers the research questions that were used in the study and seeks to provide answers based on the previous analysis. It first examines the responses from the employees' perspective and then considers the managers' perspective.

- RQ 1. What is the understanding of the requirements regarding cloud services for employees and managers in the Swedish tech industry?

Employees:

The respondents of the survey indicated that employees vary in their understanding of the requirements for cloud services in the Swedish tech industry. Most respondents noted that they were satisfied with the services used in the workplace because of the added value they provide to work tasks. However, there are indications of limited knowledge regarding the requirements for approved cloud services from the IT departments. The employees generally felt confident that they did not use cloud services that were not provided by the company. Nevertheless, most employees had used several of the services mentioned in their work, indicating that they may not be aware of the company's requirements for approved cloud services. It does not however give a clear answer if the individual services were CBSIT or not as the question design in the survey is not adequate to make this conclusion. Still, it can be seen as unlikely that several services all have licenses for the employees, especially if they provide similar functionality.

Managers:

The analysis indicates that managers from the Swedish tech industry consider security aspects as the primary concern when it comes to the requirements for cloud services. They mention the risks associated with sharing confidential information through these services and the potential for malicious activities. Managers also highlight the issues related to data ownership requirements and the legal consequences associated with them. They lack strategies to address knowledge of data ownership. There are also indications from the managers that employees who use external cloud services are not

adhering to organizational policies or legal requirements. However, there are varying opinions on how to address these issues, with some respondents favouring stricter policies while others see room for improvement in the existing ones. Lack of standardization, inadequate training for CBSIT and limited awareness of the consequences also seem to impact the understanding of the requirements for cloud services.

- *RQ 2. What are the consequences for employees who make use of cloud service solutions like Cloud-Based Shadow IT?*

Employees:

The consequences for employees using CBSIT are tendencies that leads to increased productivity, ease of setup, and better performance of work tasks. These services also offer flexibility and provide alternative options when current IT solutions are inadequate. Employees generally appreciate cloud services, even if they are considered as CBSIT. However, there are negative consequences to consider, according to the respondents. The knowledge of CBSIT is generally low, which may pose risks in understanding the company's policies. Furthermore, employees may not be aware if the services they use are considered as Shadow IT. There were also mixed opinions regarding the education provided by the IT departments on this matter.

Managers:

The analysis identifies several consequences that managers note when employees rely on CBSIT. Firstly, they acknowledge the positive aspects, such as increased collaboration, productivity, and the need for services that cater to individual needs. However, there are also notable negative aspects, including data loss, information silos between departments, and the risk of non-compliance. Excessive dependence on external cloud services can also lead to collaboration issues if the service experiences downtime or if different departments use incompatible services.

- *RQ 3. Which factors are important for employees to understand and comply with the policies in place?*

Employees:

From the employees' perspective, based on the survey, the most significant factor seems to be a general lack of awareness about CBSIT and its policy implications. Other factors can also affect this understanding. Insufficient IT solutions are another factor where the provided services are inadequate, leading employees to turn to CBSIT instead. The ease of use and setup of these services is also a factor that deters employees from complying with the policies. Therefore, factors such as proper education and awareness of security risks are crucial for employees to understand and comply with the policies in place.

Managers:

The analysis identifies a few factors that managers view as important for employees to understand the policies in use. Continuous education is rated as the most crucial factor to help employees make informed decisions. Awareness of security risks, data protection, compliance issues, and data ownership are also mentioned as important factors. Having access to awareness and education on the policies can help employees make well-informed decisions when faced with issues related to CBSIT.

9. Conclusion

The conclusions drawn from this study in the Swedish tech industry show that employees' awareness of the requirements for cloud services is mixed. The employees generally have positive views of cloud services, including CBSIT. However, there are indications of a lack of proper education, low awareness of approved services, and the policies of CBSIT. Managers see security issues as the primary concern that needs to be addressed for employees, focusing on risks related to data compliance, sharing of confidential documents, and data ownership. Furthermore, the usage of CBSIT can be seen to have clear benefits and risks, where employees are generally not aware of the policy implications it has. Important factors such as proper education, knowledge of security implications, and adequate IT solutions seem to be crucial for employees to understand and comply with policies. Establishing continuous education programs can also be beneficial for employees to make informed decisions when faced with these issues.

The knowledge contribution of this study is the insight into employees' and IT managers' understanding of the requirements of cloud services and CBSIT in the Swedish tech sector. The study also explores the consequences of using CBSIT and factors that can influence compliance with organizational policies. The findings aim to contribute to the existing literature on the implementation and management of cloud services in a tech environment. Further studies could focus on specific factors identified in this study, such as examining the security aspects of using CBSIT and mitigating the risks identified by the respondents. Additionally, exploring the legal implications of data compliance under GDPR and shaping appropriate strategies for compliance could be fruitful areas of research. Moreover, further studies can look at the specific factors in the understanding and awareness of CBSIT among employees and managers. Having a more focus on factors influencing better education in organizations.

9.1 Critical reflection

A critical reflection of this study is that the respondents were all part of a specific sector, the tech sector, which may limit the generalizability of the results. Furthermore, it could have explored the employees use of the specific services that were licensed in

their company in comparison to those that were not. Having this clearly given would have increased the validly and reliability of the study. The employees in this sector may also be more aware of IT policies and general technical risks compared to the general population. Another point of critique is the changing nature of cloud services, which may render the literature on the subject outdated. It would have been valuable to explore this factor further and ascertain if any implications of these changes affected the results. The study could have also proposed more practical contributions, such as specific strategies for education and security aspects. Additionally, conducting a hypothesis testing survey with more numerical data could have provided further insights that the analysis may have overlooked.

Reference list

Adedoyin, Olasile. (2020). Quantitative Research Method.

Ali, O., Shrestha, A., Osmanaj, V. and Muhammed, S. (2021), "Cloud computing technology adoption: an evaluation of key factors in local governments", Information Technology & People, Vol. 34 No. 2, pp. 666-703. https://doi.org/10.1108/ITP-03-2019-0119

Akande, Akinlolu & April, Nozuko & Van Belle, Jean-Paul. (2013). Management Issues with Cloud Computing. ACM International Conference Proceeding Series. 10.1145/2556871.2556899.

Andrade C. (2018) Internal, External, and Ecological Validity in Research Design, Conduct, and Evaluation. Indian J Psychol;40(5):498-499. doi: 10.4103/IJPSYM.IJPSYM_334_18. PMID: 30275631; PMCID: PMC6149308.

Bashari Rad, Babak & Diaby, Tinankoria & Rana, Muhammad Ehsan. (2017). Cloud Computing Adoption: A Short Review of Issues and Challenges. 51-55. 10.1145/3108421.3108426.

Behrens, S. (2009), “Shadow systems: the good, the bad and the ugly”, Communications of the ACM, Vol. 52 No. 2, pp. 124-129.

Birje, Mahantesh & Challagidad, Praveen & Goudar, R.H. & Tapale, Manisha. (2017). Cloud computing review: Concepts, technology, challenges, and security. International Journal of Cloud Computing. 6. 32. 10.1504/IJCC.2017.083905.

Bhatti, I. A., Khan, M. I., Ullah, S. M., & Khan, M. U. (2018). Software as a Service (SaaS): A Comprehensive Review. International Journal of Computer Science and Mobile Computing, 7(7), 1–6.

Bryman, A. & Bell, E. (2019). Social Research Methods (5th ed.). Oxford University Press.

BT. Research: Creativity and the modern CIO. (2015). https://newsroom.bt.com/shadow-it-inspires-a-renaissance-for-cios/ (Accessed 2023-06-18)

Calder, A. (2009, March 13). IT Governance Implementing Frameworks and Standards for the Corporate Governance of IT. IT Governance Ltd.

California Consumer Privacy Act. (2018). Retrieved from https://oag.ca.gov/privacy/ccpa (Accessed 2023-03-24)

Campbell, B. (2005). Alignment: resolving ambiguity within bounded choices. In Paper presented at the PACIS.

Chua CEH, Storey VC (2016) Bottom-up enterprise information systems: rethinking the roles of central IT departments. Commun ACM 60:66–72. https://doi.org/10.1145/2950044

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. Telematics and Informatics, 34(4), 157–170. https://doi.org/10.1016/j.tele.2017.01.008

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications.

Creswell, J. W., & Creswell, J. D. (2018). Research design: qualitative, quantitative, and mixed methods approaches (5th ed.). Los Angeles: SAGE.

Cronbach, Lee J. (1951). ”Coefficient alpha and the internal structure of tests” (på engelska). Psychometrika 16 (3): sid. 297-334. ISSN 0033-3123.

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method, 4th Edition Publisher: John Wiley & Sons Inc. ISBN: 978-1-118-45614-9

Dutta, A., Chandra, S., & Sharma, S. (2018). Cloud Computing: An Overview of Platform as a Service (PaaS). International Journal of Computer Applications, 163(2), 24–29.

European Union. (1995). European Data Protection Regulation. Retrieved from http://eur-lex.europa.eu (Accessed 2023-03-24)

Fernandez, E.B. and Yimam, D.,Towards Compliant Reference Architectures by Finding Analogies and Overlaps in Compliance Regulations. E-Business and Telecommunications (ICETE), SCITEPRESS, vol. 4, pp. 435-440, 2015.

Fuerstenau, D & Rothe, H. (2014). Shadow IT Systems: Discerning the Good and the Evil. ECIS 2014 Proceedings - 22nd European Conference on Information Systems.

GlobalNewswire. (2019). Enterprise IT Focused on Moving More Workloads to Cloud in 2019. Retrieved from https://www.globenewswire.com/news-release/2019/01/17/1701128/0/en/Enterprise-IT-Focused-on-Moving-More-Workloads-to-Cloud-in-2019.html (Accessed 2023-05-20)

Gigliotti, Larry & Dietsch,. (2014). Does Age Matter? The Influence of Age on Response Rates in a Mixed-Mode Survey. Human Dimensions of Wildlife. 19. 10.1080/10871209.2014.880137.

Gozman, D., & Willcocks, L. (2019). The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. Journal of Business Research, 95, 449-459. https://doi.org/10.1016/j.jbusres.2018.06.006

György, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. Paper presented at the ECIS.

Géczy, Peter and Izumi, Noriaki and Hasida, Koiti, Cloudsourcing: Managing Cloud Adoption (2011). Global Journal of Business Research, Vol. 6, No. 2, pp. 57-70, 2012, Available at SSRN: https://ssrn.com/abstract=1945858

Haag, S., & Eckhardt, A. (2017, October 4). Shadow IT. Business & Information Systems Engineering, 59(6), 469–473. https://doi.org/10.1007/s12599-017-0497-x

Höst, M., Regnell, B., & Runeson, P. (2006). Att genomföra examensarbete. Studentlitteratur AB.

IBM. (2023.). What is Shadow IT? |. https://www.ibm.com/topics/shadow-it (Accessed 2023-06-18)

Intel. (2017). New Intel Security Cloud Report Reveals IT Departments Find It Hard to Keep the Cloud Safe. https://www.404techsupport.com/2017/03/04/intel-security-report-cloud/ (Accessed 2023-06-18)

Jones, D., Behrens, S., Jamieson, K., & Tansley, E. (2004). The rise and fall of a shadow system: lessons for enterprise system implementation. Hobart, Tasmania: ACIS.

Kleindienst, D., Nüske, N., Rau, D., & Schmied, F. (2017). Beyond Mere Compliance—Delighting Customers by Implementing Data Privacy Measures?

Lewis, A. (2016). 'LinkedIn – who owns the contacts?' Linder Myers Solicitors. Retrieved from https://www.linkedin.com/pulse/linkedin-who-owns-contacts-alan-lewis/ (Accessed 2023-06-18)

Liu, S., Yang, H., & Yang, Z. (2019). A Comprehensive Survey of Software as a Service (SaaS). IEEE Communications Surveys & Tutorials, 21(3), 2510–2530.

Marc Hulsebosch: Cloud Strife, An analysis of Cloud-based Shadow IT and a framework for managing its risks and opportunities. Retrieved from https://essay.utwente.nl/69236/1/Hulsebosch_MA_EEMCS.pdf (Accessed 2023-06-18)

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011) Cloud Computing—The Business Perspective. Decision support systems, 51, 176-189. https://doi.org/10.1016/j.dss.2010.12.006

McAfee. (2020). How to Protect Your Cloud Environment. Retrieved from https://www.mcafee.com/enterprise/en-us/resources/white-papers/wp-protect-cloud-environment.pdf. (Accessed 2023-04-01)

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18(3), 15–29. https://doi.org/10.1002/dir.20009

Mishra, Dr. Shanti Bhushan, & Alok, Dr. Shashi. (2017). HANDBOOK OF RESEARCH METHODOLOGY.

Müller, S. D., Holm, S. R., & Søndergaard, J. (2015). Benefits of cloud computing: literature review in a maturity model perspective. Communications of the Association for Information Systems, 37, 851-878.

Nasuni. (2012). Half of Employees Use File Sharing Services at Work. Nasuni. https://www.nasuni.com/news/65-survey_nearly_half_of_employees_that_use_file/ (Accessed 2023-06-18)

Netskope. (2021). Cloud and Threat Report. Retrieved from https://go.netskope.com/rs/665-KFP-612/images/2021-07-Cloud%20and%20Threat%20Report-RR-474-1.pdf (Accessed 2023-06-18)

Nordgaard, A. (2011). Räkna på urval!. 2:a upplagan. V04: Dahmström, K. Från datainsamling till rapport. 3:e upplagan. Studentlitteratur.

O'Neill, A. (2018). The Regulatory Review Process: A Tool for Effective Regulatory Development. International Bar Association.

Outsourcing Law. Industries. (2017). Retrieved from http://www.outsourcing-law.com/industries/ (Accessed 2023-05-05).

Panigrahi, Ranjit & Ghose, Mrinal & Pramanik, Moumita. (2013). Cloud Computing: A new Era of Computing in the Field of Information Management. International Journal of Computer Science Engineering (IJCSE), 2.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. MIS Quarterly, 34(4).

Ray, D. (2016). "Managing risk in light of shadow IT", Inside Counsel,

ReRez Research. (2013). Avoiding the Hidden Costs of The Cloud. Issuu. https://issuu.com/integrity_ru/docs/b-state-of-cloud-global-results-2013.en-us Accessed 2023-05-05)

Rentrop, Christopher & Zimmermann, Stephan. (2012). Shadow IT: Management and Control of unofficial IT. Proceedings of the 6th International Conference on Digital Society. 98-102.

Salcedo, H. (2014). Google Drive, Dropbox, Box and iCloud reach the top 5 cloud storage security breaches list. Hitachi. Available at: http://psg.hitachi-solutions.com/credeon/blog/google-drive-dropbox-box-and-icloud-reach-the-top-5-cloud-storage-security-breaches-list, archived at http://perma.cc/36CD-3FJV (Accessed 2023-04-18)

Saldaña, J. (2015). The coding manual for qualitative researchers. Sage Publications. ISBN 978-1-44624-736-5

SCB (2018), “Use of cloud services is increasing among enterprises”, Statistiska Centralbyrån, available at: https://www.scb.se/en/finding-statistics/statistics-by-subject-area/business-activities/structure-of-the-business-sector/ict-usage-in-enterprises/pong/statistical-news/ict-usage-in-enterprises-2018/ (accessed 12 June 2023).

Schoonembom, J., & Johnson, R.B. (2017). How to Construct a Mixed Methods Research Design. Köln Z Soziol, 69(Suppl 2), 107–131. https://doi-org.e.bibl.liu.se/10.1007/s11577-017-0454-1

Seddon, J. J. M., & Currie, W. L. (2013). Cloud computing and trans-border health data: Unpacking US and EU healthcare regulation and compliance. Health Policy and Technology, 2(4), 229–241.

Selma Gomez Orr, Cyrus Jian Bonyadi, Enis Golaszewski, Alan T. Sherman, Peter A. H. Peterson, Richard Forno, Sydney Johns & Jimmy Rodriguez (2022) Shadow IT in higher education: survey and case study for cybersecurity, Cryptologia, DOI: 10.1080/01611194.2022.2103754

Silvius, A. J., & Dols, T. (2012). Factors influencing non-compliance behaviour towards information security policies. CONF-IRM Proceedings, pp. 1-14.

Silic, M., & Back, A. (2014). Shadow IT – a view from behind the curtain. Computers and Security, Vol. 45, September, pp. 274-283.

Silic M, Silic D, Oblakovic G (2016) Influence of Shadow IT on innovation in organizations. Complex Syst Inf Model Q 8:68–80

Smith, Heather & McKeen, James. (2011). Enabling Collaboration with IT. Communications of the Association for Information Systems. 28. 243-254. 10.17705/1CAIS.02816.

Shahzad, F. (2014). State-of-the-art survey on cloud computing security: Challenges, approaches and solutions. Procedia Computer Science, 37, 357–362. https://doi.org/10.1016/j.procs.2014.08.053

Straub, D. W., Gefen, D., & Boudreau, M.-C. (2005). Quantitative Research. In D. Avison & J. Pries-Heje (Eds.), Research in Information Systems: A Handbook for Research Supervisors and Their Students (pp. 221-238). Elsevier.

Strong, D. M., & Volkoff, O. (2004). A roadmap for enterprise system implementation. Computer, 37(6), 22e9. 10.1109/MC.2004.3.

Swift, Sullivan & Stillwell, Elizabeth & Ziegler, Sianna & Cheryan, Sapna. (2015). Gender Disparities in the Tech Industry: The Effects of Gender and Stereotypicality on Perceived Environmental Fit. Conference: The National conference on Undergraduate Research 2015

TechTarget. (2019). What is Cloud Compliance? Retrieved from https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing (Accessed 2023-06-18)

TechSverige. (2023). En medlems-organisation för alla företag inom techsektorn. https://www.techsverige.se/om-oss-2/ (Accessed 2023-06-20)

Techadvisor, (2023). Best cloud storage services 2023. https://www.techadvisor.com/article/723415/best-cloud-storage.html#:~:text=Table%20of%20Contents%201%201.%20Google%20Drive%20%E2%80%93,Box%20%E2%80%93%20Best%20for%20business%20...%20Fler%20objekt (Accessed 2023-06-21)

Techradar, (2023). Best online collaboration tools of 2023. https://www.techradar.com/best/best-online-collaboration-tools (Accessed 2023-06-21)

VasanthaAzhagu, A. Kannaki and J. M. Gnanasekar. “Cloud Computing Overview, Security Threats and Solutions-A Survey.” Proceedings of the International Conference on Informatics and Analytics (2016): n. pag.

Walterbusch, M., Fietz, A., & Teuteberg, F. (2017, July 10). Missing cloud security awareness: investigating risk exposure in shadow IT. Journal of Enterprise Information Management, 30(4), 644–665. https://doi.org/10.1108/jeim-07-2015-0066

Wafa'a Kassab, Khalid A. Darabkh (2020). A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and

recommendations. Journal of Network and Computer Applications, Volume 163, https://doi.org/10.1016/j.jnca.2020.102663.

Walters, R. (2013, April). Bringing IT out of the shadows. Network Security, 2013(4), 5–11. https://doi.org/10.1016/s1353-4858(13)70049-7

Weill, P., and Ross, J. W. 2004. IT Governance: How top performers manage IT decision rights for superior results, Boston, MA: Harvard Business School Press.

Wikin & Sjöblom. (2017). Sweden data protection overview. Retrieved from https://www.dataguidance.com/notes/sweden-data-protection-overview (Accessed 2023-04-13)

Wienclaw, R.A. (2021) 'Confidence Intervals', Salem Press Encyclopedia [Preprint]. Available at: https://search-ebscohost-com.e.bibl.liu.se/login.aspx?direct=true&AuthType=ip,uid&db=ers&AN=89185376&lang=sv&site=eds-live&scope=site (Accessed 18 June 2023).

Ya-Ching Lee (2019). Adoption Intention of Cloud Computing at the Firm Level. Journal of Computer Information Systems, 59(1), 61-72. DOI: 10.1080/08874417.2017.1295792

Zhou, C., Barati, M., & Shafiq, O. (2023). A compliance-based architecture for supporting GDPR accountability in cloud computing. Future Generation Computer Systems, 145, 104–120. https://doi.org/10.1016/j.future.2023.03.021

Appendix

Definition: Software as a service

Software as a service (SaaS) is a method that lets organizations run their software through the cloud which enables access through client login and client computers. It enables licenses of software to be used for organization to certain authorized person and usually stores the program to be accessed when the authorized person accesses their account. It enables organizations to have the program through the internet without having the need to install it locally. It eases the need to gain knowledge of certain software issues and the management of the hardware on which it is installed. Research has seen that SaaS has advantages for organization when being cost effective and being able to spend less resources of having IT-maintainers. It can also be seen as more secure than traditional methods with a provider who specializes in its security. Furthermore, it has shown that businesses that have implemented SaaS are shown to be able to spend more time on central business activities without having the need to worry about IT resources. Freeing up more time for other business needs (Bhatti et al 2018).

Businesses switching over to SaaS based solutions have seen its benefits since gaining popularity, but it also has its drawbacks. Since SaaS relies on the uptime of the service provider. A downtime from the provider can lead to major consequences for a business day to day operations. Another issue is that a firm can have little understanding of the troubleshooting process of a service they have gotten, resulting in processes of troubleshooting outside the organization (Liu et al. 2009).

Definition: Platform as a service

Platform as a service (PaaS) uses hardware and software to be provided through the cloud by using the providers established IT-architecture. It is mainly entered through a web browser and enables clients to usually perform complex tasks in a more effective way. Typical applications on these platforms can be software development, team development and testing programs (Bhatti et al 2018).

The benefits of SaaS have given more efficient solutions for businesses as more scalability, speed, and reduction of costs. It enables programmers to deliver their applications in a quicker way while also being able to display them with ease. Laying focus off on spending time on infrastructure and instead focusing on developing software (Dutta et al 2018)

Definition: Infrastructure as a service

Infrastructure as a service (IaaS) takes it one step further where companies can rent out infrastructure from providers to fill their own needs. This can be servers, storage devices, equipment. Usually, it is provided through a subscription-based module or through a pay per need usage. It makes it possible for businesses to easily change their IT needs based on the current and future. It provides a solution for organizations that do not wish to spend their own time or resources to establish their own hardware and infrastructure. It is seen as a cost-effective solution as well as a flexible one (Bhatti et al 2018).

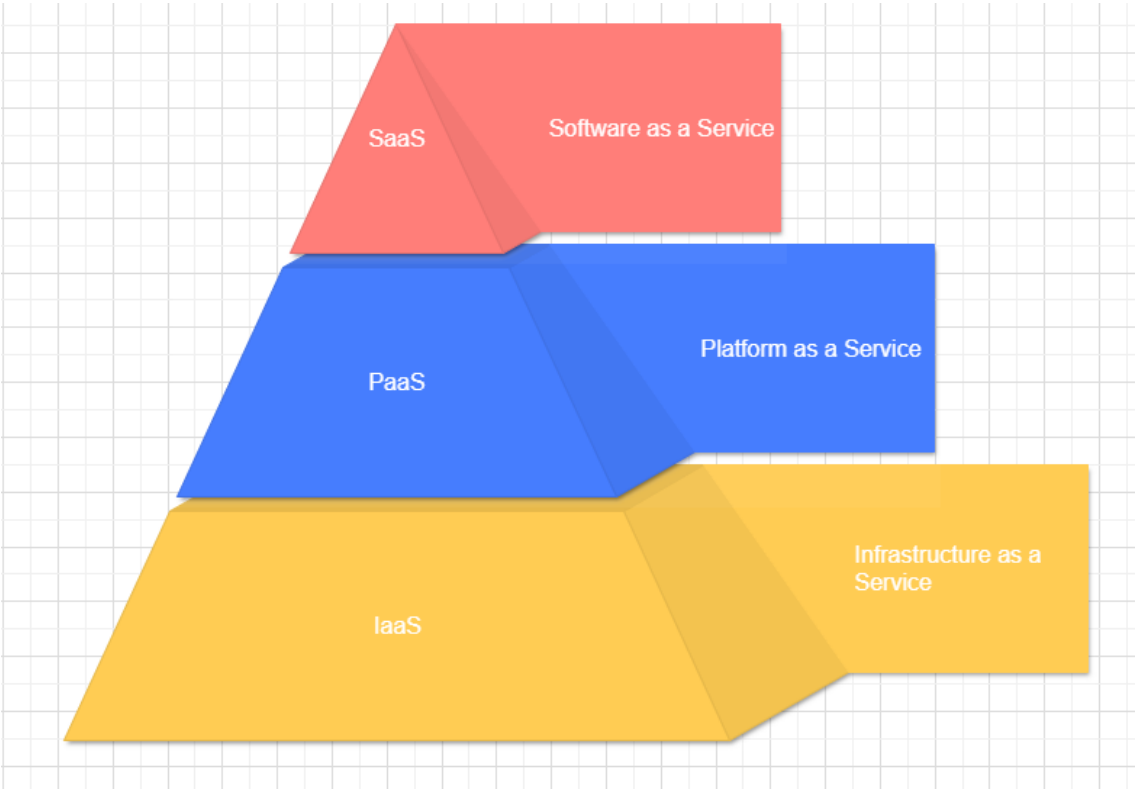

Figure 1. Cloud Computing Services

Deployment models

There are four main models for that businesses operate when dealing with cloud computing.

Public Cloud:

A public cloud is the most frequent model that businesses use. It consists of using a third-party service to operate the cloud over the internet. The offers consist of primarily a model where companies pay for what they use in a pay-as-you-go model. Common public cloud providers are Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP). They operate large scale centers that offer various services across the world.

Advantages	Disadvantages
Great availability	Little opportunity for customization
Easy to scale	Potential security issues
Little to no maintenance	Less control
No upfront cost	Being dependent on a provider

Private Cloud:

A private cloud uses either organizational resources or resources from a third-party provider to set up its cloud. In contrast to public cloud, this option provides a more flexible approach for the business. The management of the cloud is handled by the organization or it's provider. It enables easier scalability while also enabling more control operations and increased security.

Advantages	Disadvantages
Great control	Higher cost
Greater security than public option	More need to manage
Better flexibility for resources	Lower potential to scale compared to public
Easier to comply with regulations	Harder to access external resources

Hybrid Cloud:

A hybrid cloud solution is a mix of a public and private cloud services which in addition uses infrastructure on site for the organization. Establishing a relationship between all three to create a cloud environment. It enables management to adjust needs for security, scalability, customization, and control to their own liking without the restrictions imposed on public and private alone.

Advantages	Disadvantages
Flexible	Harder to set up
Secure	Higher cost
Easy to scale	Harder with security
Easy to customize	More complex data handling

Timeplan

Week	Plan
4 & 5	Essay plan
6	Essay plan
7 & 8	Literature review
9	Literature review & establishing interview protocol.
10 & 11	Literature review, completing questionnaire for survey
12	Start sending out survey
13 & 14	Interview and handling of data
15	Finish data, write method used,
16	Analysis
17	Discussion and prepare for laying forward
18	Conclusions
19 - 21	Conclude paper
22	Finish paper and prepare for turning in
23	Prepare presentation and turning in final essay

Avsnitt 1 av 4

Study about external Cloud-Based IT services in a workplace

Thank you for taking the time to participate in my master's thesis survey. The purpose of this study is to explore the impact of external Cloud-Based IT on workplaces and to gather employees' experiences of using it. Specifically, the study focuses on the use of external Cloud-Based IT services that are not directly approved by the IT department. Your participation in this study is greatly appreciated and the survey should only take around 5-10 minutes to complete.

The answers you provide in this survey will be used to help IT managers make better decisions regarding the use of external Cloud-Based IT services. It is important to note that participation in this study is fully voluntary and all answers provided will be kept confidential.

Thank you again for your participation in this research.

What is your gender? *

- ○ Male
- ○ Female
- ○ Other
- ○ Prefer not to say

Avsnitt 2 av 4

Questions about Cloud-Based IT-services

Beskrivning (valfritt)

How frequently do you use Cloud-Based IT services in your work tasks? *

	1	2	3	4	5	6	7	
Not very often	○	○	○	○	○	○	○	Very often

How easy is it to access and use the cloud services provided by your company? *

	1	2	3	4	5	6	7	
Not very easy	○	○	○	○	○	○	○	Very easy

How strongly do you agree with the statement "I am satisfied with the current Cloud-Based IT services in my workplace"? *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

How strongly do you agree with the statement "The Cloud-Based IT services provided in my workplace fulfill the requirements for my work tasks"? *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

How strongly do you agree with the statement "I can easily get help with the Cloud-Based IT services from my IT department"?

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

Efter avsnitt 2 Fortsätt till nästa avsnitt ▾

Avsnitt 3 av 4

Cloud-Based Shadow IT

Beskrivning (valfritt)

How often do you use cloud services for work purposes that are not officially approved or provided by your company (e.g., personal Google drive account)? *

	1	2	3	4	5	6	7	
Not very often	○	○	○	○	○	○	○	Very often

Have you used any of these services in your work tasks? (one or more) *

- [ ] Dropbox
- [ ] ICloud
- [ ] Google Drive
- [ ] OneDrive
- [ ] MEGA
- [ ] Trello
- [ ] Slack
- [ ] Zoom
- [ ] None

How comfortable are you with using the above services for work-related tasks? *

	1	2	3	4	5	6	7	
Very uncomfortable	○	○	○	○	○	○	○	Very comfortable

Do you consider these services a good addition in your everyday work tasks? *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

How strongly do you agree with the statement, "I have needed to use these services because of insufficient IT solutions"? *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

What factors influence your decision in using these services for work purposes? (one or more) *

- [ ] Productivity
- [ ] Ease of use
- [ ] Flexible
- [ ] Collaboration
- [ ] Easier than implementing new internal services
- [ ] Lack of support for internal services
- [ ] Customer experience
- [ ] Other

If other option, please state the reason

Kort svarstext

Are you familiar with the company's policies around the use of these services for work-related tasks? *

	1	2	3	4	5	6	7	
Very unfamiliar	○	○	○	○	○	○	○	Very familiar

Efter avsnitt 3 Fortsätt till nästa avsnitt

Avsnitt 4 av 4

Shadow IT

Shadow IT is the use of hardware, software, and IT services which do not have direct approval from the IT department. This study focuses on the cloud-based side of Shadow IT.

How familiar are you with the concept of Cloud-Based Shadow IT? *

	1	2	3	4	5	6	7	
Very unfamiliar	○	○	○	○	○	○	○	Very familiar

How strongly do you agree with the statement "I think my IT department educates me about the use of external based IT cloud services and the implications they bring"? *

	1	2	3	4	5	6	7	
Strongly Disagree	○	○	○	○	○	○	○	Strongly Agree

How strongly do you agree with the statement, "When using these services I make sure to think about the information I'm sharing"? *

	1	2	3	4	5	6	7	
Strongly DIsagree	○	○	○	○	○	○	○	Strongly Agree

Have you ever experienced a data breach or security incident because of any of these services in the workplace? *

- ○ Yes
- ○ No
- ○ Maybe