Multi-Cloud Information Security Policy Development

A conceptual framework for developing information security policies in a multi-cloud context

SINDRE PEDERSEN FOSSER
THOMAS ØREN

SUPERVISOR
Wael Soliman

University of Agder, 2023
Faculty of Social Sciences
Department of Information Systems

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	Ja
2.	**Vi erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	Ja
3.	Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	Ja
4.	Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	Ja
5.	Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	Ja
6.	Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	Ja
7.	Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet.	Nei

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	Ja
Er oppgaven båndlagt (konfidensiell)?	Nei
Er oppgaven unntatt offentlighet?	Nei

Acknowledgements

We would firstly express gratitude towards our thesis supervisor Associate Professor Wael Soliman at the Department of Information System at University of Agder. The continuous feedback and engagement throughout the semester pushed us towards the finish line. Further, the constant constructive critiques and tips, challenged us to make a product we could be proud of.

Lastly, we want to show courtesy to the willing respondents. To take time of their day to answer our questions, resulting in our empirical findings to be valid and relevant. These experts gave us insights to what research papers could not give us with experience and practical information.

Thank you!

Kristiansand,
June 2nd, 2023

Sindre P. Fosser

Thomas Øren

Sindre Pedersen Fosser

Abstract

Organizations' ever lasting desire to utilize new trending technologies for optimizing their businesses have been increasing by the years. Cloud computing has been around for a while, and for many became a vital part of their day-to-day operations. The concept of multi-cloud has allowed organizations to take advantage of every cloud vendor's best services, hinder vendor lock-in, resulting in cost optimization, and resulting in more available services. With every new technology, there are new vulnerabilities ready to be exploited at any time. As there is little prior research regarding this field, threat actors can exploit an organization's ignorance on important challenges such as interoperability issues, implementing multiple vendors resulting in losing track of their services, and the lack of expertise in this newly founded field. To alleviate such issues, one approach could be to develop information security policies, hence our research question for the thesis: *How to develop information security policies in a multi-cloud environment with considerations of the unique challenges it offers?*

To uncover the research question, we have conducted a systematic literature review followed up by a qualitative research approach. This has resulted in six semi-structured interviews from respondents with a variety of experience within the multi-cloud realm. The most prominent findings from this exploratory study has been the focus of thoroughly planning the need of a multi-cloud and information security policies, as well as applying a top-down approach for the policy development phase. This gives a more holistic view over the process, and additionally having the right competence is important. An interesting finding was that multi-cloud on paper should prevent the vendor lock-in issue, but in reality may provoke the matter. Using the tools and services provided by the cloud service providers may enhance the development of information security policies, but proves to be difficult in multi-cloud as the problem of interoperability hinders this. Lastly, reviewing policies becomes more time-consuming and resource heavy in a multi-cloud because of the frequent updates and changes in technology, which has to be monitored. This research presents a conceptual framework, which by no means is a one-size-fits-all solution, but raises discussion for future work in this field.

Keywords: ***multi-cloud, information security policy, development, cybersecurity, cloud computing***

Contents

List of Figures

List of Tables

List of Abbreviations

2FA Two-factor Authentication

API Application Programming Interface

CIA Confidentiality Integrity Availability

COBIT Control Objectives for Information and Related Technologies

CSP Cloud Service Provider

DDoS Distributed Denial of Service

GBRAM Goal-Based Requirements-Gathering

GDPR General Data Protection Regulation

IaaS Infrastructure as a Service

IAM Identity and Access Management

ISMM Information Security Maturity Model

ISO International Organization for Standardization

ISP Information Security Policy

ISPA Information Security Policy Architecture

MCaaS Multiple Clouds as a Service

NSD The Norwegian Center for Research Data

NSM The Norwegian National Security Authority

OLA Operational Level Agreement

PaaS Platform as a Service

PFRIES Policy Framework for Interpreting Risk in eCommerce Security

PRISMA Preferred Reporting Items for Systematic Reviews and Meta-Analyses

QoS Quality of Service

SaaS Software as a Service

SARC Security Activity Resource Coordination

SLA Service Level Agreement

SLR Systematic Literature Review

TLS Transport Layer Security

Chapter 1

Introduction

The rapid growth of digital transformation have shifted enterprises' approach of utilizing their infrastructure over the past decade. The migration over to the cloud have made enterprises more efficient with quicker results and simultaneously lower the costs (Hong et al., 2019). Additionally, there have been new technologies such as fog, edge, and multi-cloud solutions. Multi-cloud environments, characterized by the simultaneous use of multiple cloud service providers, offer increased flexibility, scalability, and cost-efficiency. With this drastic change over time there have emerged new issues to be mitigated by enterprises, as threat actors are always in a continuous growth. Developing robust security policies becomes crucial to safeguarding organizations against various threats and vulnerabilities inherent in the multi-cloud landscape. From a global perspective, Flexera (2022) presented a statistic over organizations which operate in cloud, that 89 percent have adopted some sort of multi-cloud setup. Statista (2023) showed a 188 percent increase in revenue of the public cloud market in Norway from 2018 to 2023, this implies that Norwegian enterprises use and rely on cloud computing for their operations today.

Organizations have seen the benefit of migrating to a multi-cloud environment to gain cost optimization and use each cloud vendors' best applications. Additionally, with all the breaches reliant on a singular cloud, which in turn stops the whole organization's business, have executives worried of vendor lock-in. Albeit this multi-cloud proposition clearly delivers assorted benefits, cyber threats continue to adapt and be more complex than ever. A report by VentureBeat presented that 69% have expressed they have experienced some sort of breach or exposure as a result of multi-cloud configuring (VentureBeat, 2022). The most common cloud cyber attacks are also still a highly likely outcome with the likes of ransomware, supply chain attack, DDoS, phishing, etc. With multiple cloud vendors, attackers can now exploit bad configuring between the cloud providers and have even a larger attack surface. The reality is that companies are now in front of a great challenge in protecting their services against persistent threats from every corner - some would call it a storm for data breaches.

With this in mind, we pose the following research question: *How to develop information security policies in a multi-cloud environment with considerations of the unique challenges it offers?*

The primary objective with this study is to gain a more in-depth understanding over how this new technology affects organizations today. Furthermore, how one can develop their own policies that can enhance the overall security. We aim to create a conceptual framework which will lay out the whole policy development life cycle, and further include best practices and recommendations.

1.1 Rationale and motivation

This study aims to investigate how enterprises in Norway develop their security policy when managing multiple cloud service providers. To our best knowledge, there have not been any exclusive studies regarding this topic yet, which intrigued our curiosity. The multi-cloud trend have continuously grown over the past years, with a study from Flexera (2022) showed that a whopping 89% of organizations that operate in cloud uses multi-cloud on a global level. This gives us a strong indication that this field is highly relevant, and should be investigated further. For narrowing down our study even more, we decided to incorporate security policies, which are crucial for any organization. Paananen et al. (2020) reveals that there is a surprisingly small amount of research on this topic, despite the fact that it is generally thought to be the basis of information security. There are no specific templates nor framework for creating security policies for a multi-cloud system. We can firstly see if the policy development methodology could be the same or if it is necessary for specific policies. Although there are no studies specifically looking at security policy development in a multi-cloud context, there are research papers that explains the general challenges and multi-cloud complexity well (Hong et al., 2019; Petcu, 2013). Schrama (2021) wrote a Master's thesis around governance management in multi-cloud. Wiener and Saunders (2014) discussed potential multi-sourcing models and that multi-cloud could force cloud vendors to collaborate unwillingly. Both Elliott et al. (2018) and Ranjan (2014) addressed a huge challenge in multi-cloud, which is interoperability, and how cloud agnostic security and centralized APIs can resolve this issue.

1.2 Report structure

Chapter 1: Introduction - Gives the reader an overview over the topic and problem

Chapter 2: Background - Presenting the literature review process and findings to end with our conceptual framework

Chapter 3: Research approach - Showcases why the chosen research approach are suitable for this study. Further, includes research design, data collection, interview, data analysis, and limitations & challenges

Chapter 4: Findings - Where we display our empirical findings from the interviews

Chapter 5: Discussion - This is where we deliberate regarding the empirical findings by theoretical -and practical implications, followed up by any further work and potential limitations

Chapter 6: Conclusion - Determine a conclusion and presenting main findings

Chapter 2

Background and related work

In this chapter we will discuss our literature review process, which includes our method of choice, inclusion criteria, the process of our literature search, as well as the screening process and extracting and analyzing. The aim to discover development methods in multi-cloud is split into three sub-questions to help us conduct the literature review more easily. Afterwards, we will discuss all the related research in this chapter, which will serve as the foundation for our conceptual framework and the thesis onwards.

2.1 Literature review

A systematic literature review (hereafter referred to as SLR) is utilized to identify, evaluate, and interpret all of the available research data relevant to a certain predetermined research question, problem area, or something of interest to the people conducting the SLR (Kitchenham and Charters, 2007). By looking at previous research, we can identify gaps while gaining an understanding of the breadth and depth from already existing works. Afterwards, we analyze and summarize relevant literature to investigate our own hypothesis, or develop new theories (Paré et al., 2015). Our goal with conducting this SLR was to gain a better understanding of multi-cloud architecture, as well as its security issues, best practices, potential research gaps, and current solutions. All of the above was to gain an extensive understanding over how the multi-cloud environment works in relation to the potential vulnerabilities. With this in mind, we want to find out how to develop security policies linked to multi-cloud systems. To develop adequate information security policies, it is essential to have a satisfactory perspective over the architecture and threat landscape for the given subject. Based on this we have formulated the research question below, which will guide the entire SLR process (Kitchenham and Charters, 2007):

RQ How to develop information security policies in a multi-cloud environment with considerations of the unique challenges it offers?

As we mentioned, we need a deeper understanding of the multi-cloud model and what element goes into a security policy development process. Furthermore, we can break down the research question into several smaller and simpler ones to guide our SLR in the direction we aim for.

1. What is a multi-cloud system?
2. What are the security concerns that are unique for a multi-cloud system?
3. How to develop ISPs?

The goal of the first sub-question is to properly define the terminology of multi-cloud systems, as there are multiple comparable terms that describe similar systems. The second one's aim is to identify security concerns that are unique to a multi-cloud system to give us a better understanding of what an ISP should include to help mitigate these issues. Lastly, we need to understand the development process for ISPs, and if it is plausible to incorporate these methodologies into a multi-cloud context.

2.1.1 Method

At the start of our SLR process, the research questions were somewhat general and not specific enough. We had defined our problem area as "multi-cloud security", but we lacked the required knowledge in this area to define a proper research topic. We started a broad search to create a theoretical foundation, to then narrow it down the further we proceeded in our research. It has been an iterative process, eventually ending up at our topic of "developing security policies for a multi-cloud system". Following an SLR approach helped us identify relevant papers and articles, which were then used to "snowball" into further interesting literature.

Our process is inspired by the model presented by Xiao and Watson (2019), which is illustrated below. Having a clear guideline for the SLR ensured that we were able to collect relevant literature to extract and analyze. It is also an appropriate approach for us because we are aiming to produce a conceptual framework, which is one of the main reasons to perform an SLR according to Kitchenham and Charters (2007).

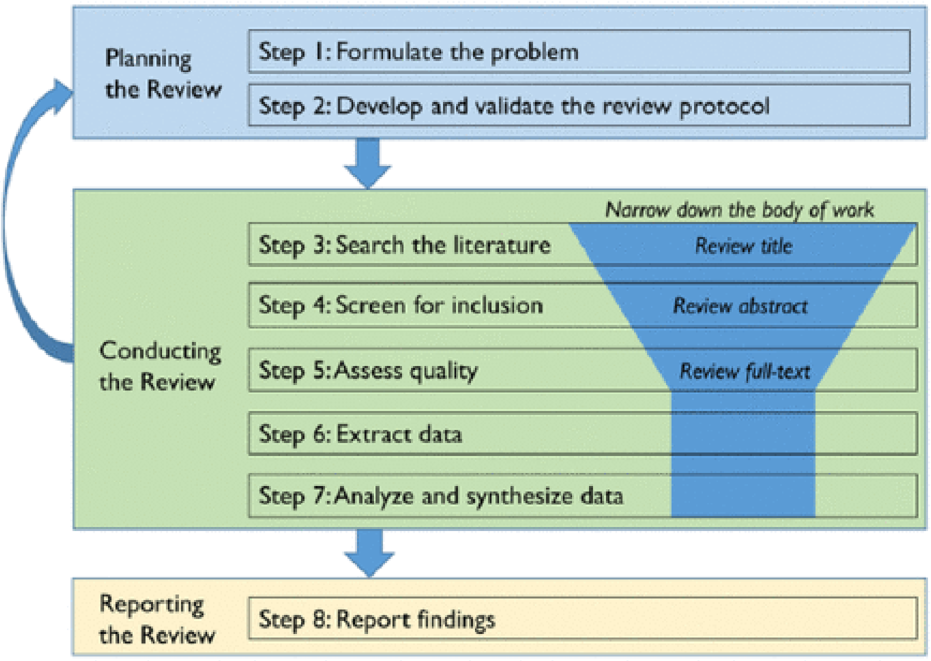
Planning the Review
Step 1: Formulate the problem
Step 2: Develop and validate the review protocol
Narrow down the body of work
Step 3: Search the literature
Review title
Step 4: Screen for inclusion
Review abstract
Conducting the Review
Step 5: Assess quality
Review full-text
Step 6: Extract data
Step 7: Analyze and synthesize data
Reporting the Review
Step 8: Report findings

Figure 2.1: The process of a systematic literature review (Xiao and Watson, 2019)

2.1.2 Literature search

The literature search is the subsequent step after developing and refining the research questions. This process involves gathering all the relevant material that will be used later in the review. This essentially means that the set quality of the literature review is greatly affected by this phase. Hence, the need for a systematic method of searching the literature.

Channels for literature search

There are three major sources we used to find relevant literature: electronic databases, backward -and forward searching.

Electronic databases: Probably the most common used method of sourcing literature would be through electronic databases/libraries. There are numerous databases one can utilize, and no single database contains all the literature we need. Therefore, a systematic search for literature should come from various databases (Xiao and Watson, 2019). We wanted to acquire a comprehensive list of literature, which is why we decided to utilize the most commonly used databases for academic and scientific journals. Additionally, since the domain of cybersecurity/information technology is an interdisciplinary one, looking at databases targeting exclusively these fields would be to our detriment. Therefore, we decided to predominantly use these databases; Web of Science Core Collection, Google Scholar, Scopus, and IEEE Xplore.

Backward and forward reference searching: When one have found relevant literature, a *backward search* can be executed to discover similar articles referenced in the original paper. By using this method, we can gain a better understanding of the author's influence of theories and ideas. This is frequently used for literature searching, as it can exponentially increase the amount of relevant literature, creating a snowball effect. We were using this method persistently throughout our literature search process and found additional relevant papers that could have been difficult to discover with just a database search.

On the contrary, a *forward search* is the method to identify citations of the paper after it has been published. This can be used to expand upon the knowledge on the topic by follow-up studies, as well as classifying new findings or developments. This method is also being called by many, "snowballing".

Keywords

When searching for literature, the keywords should be derived from the research question(s) (Xiao and Watson, 2019). To do this, the research question can be resolved into multiple concept domains (Kitchenham and Charters, 2007). Looking at our research question, it can be dissected into a few different domains: How to develop a multi-cloud specific ISP?, What is a multi-cloud system?, What are the security concerns that are unique for a multi-cloud system? and How to develop ISPs?. The logical domains in our case are: "Multi-cloud", "challenges", "security", and "policy". With a these domains established, we can perform a preliminary search using these terms as starting keywords. Searching through the selected databases with a combination of these keywords produces some relevant literature, but further adjustments are needed. For adjustments, synonyms, abbreviations, alternative spellings and related terms of the original statement can be used (Kitchenham and Charters, 2007), as illustrated in the table below.

Table 2.1: Keywords table

Keyword	**Related terms**
Multi-cloud	Cross, hybrid, inter, federated
Security policy	CSP, Information security policy (ISP), Policy development, methodology
IS governance	Compliance, SLA, Direct-Control
Architecture	Framework, system, infrastructure, model
IT sourcing	Multi-sourcing, forced coopetition
Interoperability	Cloud-agnostic, portability, standardization

A good balance between inclusiveness and precision is important (Wanden-Berghe and Sanz-

Valero, 2012). Using broader keywords may fetch more results, but on the other end the search might produce articles that are insignificant to our given study. Contrary, using excessively defined keywords can improve the search accuracy with precise relevant articles, but will leave out potential other interesting articles. As recommended by Wanden-Berghe and Sanz-Valero (2012), we went for an inclusive strategy at the start of our SLR process, and further defined our keywords in the later stages to maximize the data collection. After repeated searches that resulted in the same references appearing with little to no new results, we concluded that we should stop the literature search. We utilized the boolean function from the search engines to refine our searches more inclusively e.g.: ("∼multi-cloud") or ("multi-cloud" AND "policy"). This was useful as the term multi-cloud is heavily used interchangeable between the hybrid, cross, and inter.

2.1.3 Screen for inclusion

After all the research has been compiled, further screening of every article for inclusion or exclusion should be conducted (Xiao and Watson, 2019). We performed a two-step process to ensure efficiency: Firstly, read the title, then abstract (and conclusion if abstract does not provide enough information) of each article to swiftly make a judgment on whether it should be included. Second, read the full text to assess the quality. We decided if we were ever in doubt regarding the inclusion of an article, that we should be inclusive and later remove the paper if we saw it not fitting.

Inclusion criteria

The inclusion and exclusion criteria should be constructed with the research question in mind (Kitchenham and Charters, 2007). This means that any research that is unrelated to the research questions should be excluded from further analysis (Xiao and Watson, 2019). Any and all literature that has no relation to multi-cloud or security policies should be ignored. Furthermore, the criteria should be practical (Okoli and Schabram, 2010). Papers should be easy to apply and give an understanding of our process in selecting research material, while also providing guidelines on what type of materials are appropriate for our project. With all this in mind, our given criteria are:

- The articles must be related to our research questions (e.g. information about multi-cloud security issues, ISP development articles)
- Must be written in a language we can understand (English or Norwegian)
- Articles related to multi-cloud must have been published by latest in 2013, while policy development related ones can be published earlier
- Papers with more citations are to be prioritized when similar ones appear

2.1.4 Screening procedure

In accordance with the search procedure and the established selection criteria, we performed a full-text review of all the remaining eligible articles as our screening process to include or exclude literature.

Firstly we conducted a preliminary search were we used various keyword strings as mentioned before, to find our first potential papers for reviewing. As we started the searching process separately, we found out that there were some duplicate articles, which after removal resulted in 173 articles left. The remaining were excluded through the relevance of the title, while the rest would be up for an abstract read through, and in some cases conclusion as well. After this abstract screening we were left with 25 articles. These were then up for a full-text assessment, to validate the relevancy of our topic. In this process we also found new articles to collect via snowballing. These articles would be difficult to find otherwise, but were useful as it gave us a broader understanding over the authors' inspirations and thinking. After this process we left out 14 papers, but added 9 articles. Finally, after the screening procedure was done, the SLR ended up with 23 articles in total. To illustrate our process, we created a Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram which is shown below.

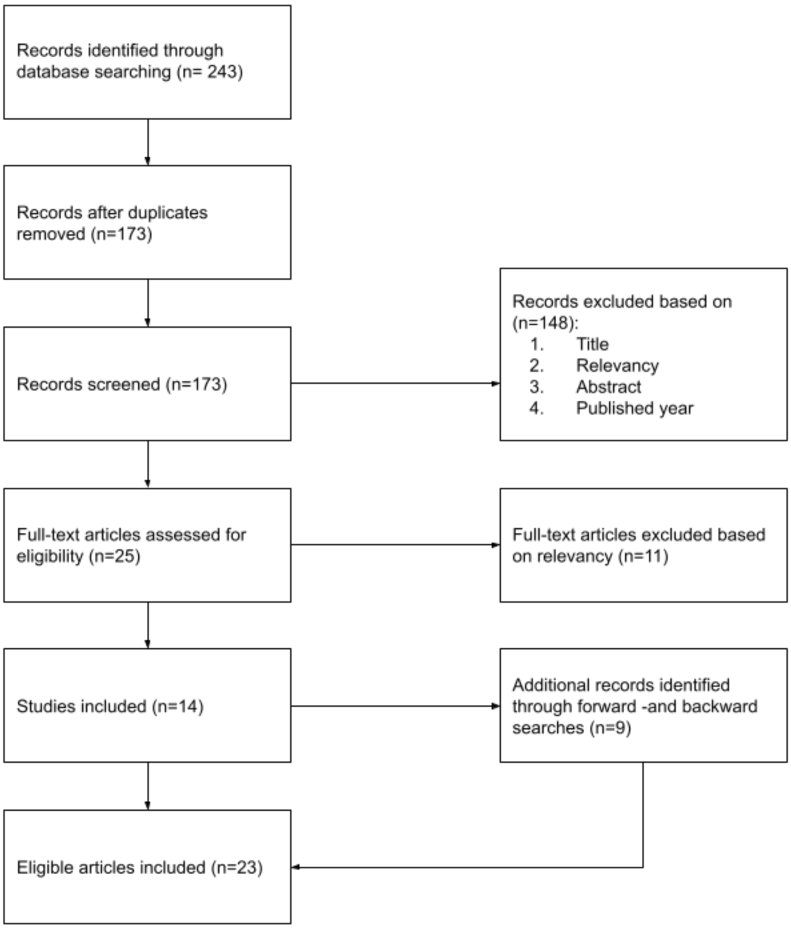
Records identified through database searching (n= 243)
Records after duplicates removed (n=173)
Records screened (n=173)
Records excluded based on (n=148):
1. Title
2. Relevancy
3. Abstract
4. Published year
Full-text articles assessed for eligibility (n=25)
Full-text articles excluded based on relevancy (n=11)
Studies included (n=14)
Additional records identified through forward -and backward searches (n=9)
Eligible articles included (n=23)

Figure 2.2: Literature search and evaluation for inclusion

This process was iterative and had a steep learning curve, where we in the beginning had little to no knowledge regarding the topic. The more understanding we got, the thesis matured, and we could filter in or out more relevant articles to our SLR. The multi-cloud realm is a huge topic, and as we gained the necessary basic information, we had to scope down to fit our thesis. As we could easily go through all the intricacies of the technical -and compliance details, which would take forever. After constantly resharpening our keywords and finding additional articles via snowballing, we were content with the remaining articles left.

After our screening process were conducted, we were left with 23 articles to be proceeded in the SLR. These are presented in the table presented in appendix A. This list contains the author(s), title of the paper, which database used, and which search string used.

2.1.5 Extracting and analyzing

Coding is often utilized for data extraction (Xiao and Watson, 2019). We used the analytical tool called NVivo to code all findings related to our research questions in the selected literature. Kitchenham and Charters (2007) recommends that researchers should code an article together at the start to ensure that they are on the same page when coding. We utilized this method and started out with coding a couple of articles together, then when the baseline for how we code was established, we separately coded the rest of the articles individually, sporadically discussing our findings.

2.2 IT outsourcing

This section will introduce briefly the history of IT outsourcing and the evolution into multi-sourcing and cloud computing. Furthermore, we will describe the different IT multi-sourcing models which will lead us into the discussion of multi-cloud in the next section.

2.2.1 IT outsourcing history

IT outsourcing has existed as a concept for a while, originating in the 1960s primarily focusing on hardware (Lee et al., 2003). It is the act of delegating IT related decisions, processes, or services to third parties and have them develop, manage, and administer them in accordance to prior agreements (Dhar, 2012). Lee et al. (2003) present a model that highlights the evolution of IT outsourcing and the different steps in such arrangements, with the first being 'make or buy' to the last 'partnership'. Deciding on the amount of providers falls in-between the 'scope' and 'performance' steps, which introduces the multi-sourcing concept. Multi-sourcing IT arrangements requires considerable coordination efforts and cooperation between vendor and consumer, where Operational Level Agreements (OLA) and certain sourcing models can assist with these efforts.

IT outsourcing allowed companies to focus on their core business processes instead of software development or other IT related services (Dhar, 2012). Cloud computing was the next step in the evolution of outsourcing. It has many similarities to IT outsourcing, but to understand the evolution it brought forth, Dhar (2012) highlights the differences between cloud and traditional IT sourcing. It brought customers efficient, economical, and flexible IT services along with versatile payment options. Although it was a new form of IT sourcing, it was apparent that it also brought forth complexities in regards to implementation, integration, and management of cloud computing services. Issues like security and privacy was also noticeable for the consumers (Dhar, 2012). This is important to keep in mind when discussing multi-cloud, as managing security of a single cloud is already difficult. Integrating multiple clouds from multiple vendors can only result in making it more difficult.

2.2.2 IT multi-sourcing

IT multi-sourcing can be described as "the situation where a client firm delegates IT projects and services to multiple external vendors who must, at least partly, work cooperatively to achieve the client's business objectives" (Wiener and Saunders, 2014). Bapna et al. (2010) were one of the earlier ones to address this change in the dyadic relationship between a single vendor and client. They highlight the complex coordination needed, and emphasize questions such as: how can multiple vendors deliver a seamless integrated service? Is it easy to switch to another vendor? Who is accountable in the case of a failure to deliver the service? Bapna et al. (2010) and Wiener and Saunders (2014) argue that vendors should cooperate with each other to ensure that the arrangement is fulfilled. OLAs can assist with coordination efforts, as well as the guardian vendor model.

The usage of multi-sourcing entails a slew of advantages, such as lower price, better service quality, more flexibility, lower financial risk, less lock in, and quicker access to new technology. On the other hand, there are also some downsides when utilizing multi-sourcing, which includes additional cost, it being difficult to appoint responsibility in the case of failures, poor attention to contract, and no relationship-specific investments. Some of the advantages and disadvantages are remarkably similar to using multi-cloud.

2.2.3 Multi-sourcing models

In the guardian model, one vendor acts as a guardian and relieves some of the responsibilities of managing the vendors for the client (Oshri et al., 2019). To complement the clients lack of architectural knowledge the guardian vendor can help with maintaining the architecture of the IT arrangement. It does not completely substitute the client and their governance of multiple vendors. Other articles argue that the guardian has the role of mediator, acting as a single point of contact, facilitating the coordination and cooperation efforts between other vendors on the client's behalf (Bapna et al., 2010; Schmidt and Suomi, 2018; Wiener and Saunders, 2014). Wiener and Saunders (2014) presents other types of multi-source models which can be seen in figure 2.3. The mediated model is as mentioned earlier, the single point of contact for coordination efforts. In the direct model, the client arranges everything themselves and governs the relationships without any assistance from other entities. This takes considerable effort, and can result in having to take measures such as redesigning business processes, or creating vendor interfaces (Alpar and Polyviou, 2017). In both of these models, the competition and cooperation between vendors is on the lower to moderate side of the spectrum. This is because the vendors operate on their own dedicated area of responsibility and cooperation is at a surface level. On the other hand, with the direct-overlapping model the vendors operating area is overlapping and the interdependent actors must cooperate at a more in-depth level. This brings about the so-called forced coopetition, producing higher levels of competition and cooperation (Wiener and Saunders, 2014).

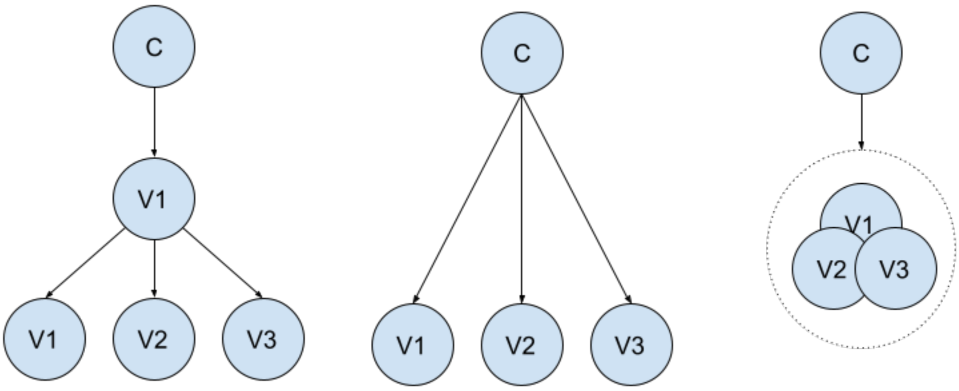

Figure 2.3: Mediated, direct, and direct-overlapping multi-source models. (Wiener and Saunders, 2014)

Another model is the partnership-oriented model (Schmidt and Suomi, 2018). It is somewhat related to the direct-overlapping model, but the main difference between them is the lower amount of competition in the partnership-model. Competition is only limited to the bidding phase in the start, where firms are selected to perform tasks based on their abilities. The main focus is on creating a liaison between vendors to eventually create a long-standing partnership (Schmidt and Suomi, 2018).

2.3 Exploring multi-cloud

To gain a better understanding of the multi-cloud environment and answer our research question, we looked at the different terms that describe a setup that uses multiple clouds, as well as some of the security issues that present themselves in a multi-cloud model. Furthermore, we addressed the problem of interoperability.

2.3.1 Defining multi-cloud

There are numerous terms used to describe different variations of a multi-cloud architecture, such as federated cloud, hybrid cloud, inter-cloud, cross-cloud, and so on. We will attempt to categorize all the separate terms to ensure that both us and the readers get a better understanding of how they differ from each other.

Multi-cloud

The term multi-cloud refers to the usage of multiple independent cloud computing services (Petcu, 2013; Rosian et al., 2022). The different cloud networks are combined with the purpose of fulfilling different roles to satisfy specific needs of the organization (Hong et al., 2019). All the cloud services may be utilized to differing levels, as well as having unique Service Level Agreements (hereafter referred as SLA). Petcu (2014) mentions that in a multi-cloud model, there are no prior agreements between the cloud providers to cooperate and the consumer (or a third party) is responsible for handling the coordination efforts between them which includes: directly contacting the service providers, negotiating terms of service consumption, monitoring fulfillment of SLAs, and so on. Furthermore, they mention that there are two different categories of multi-cloud: Service based, or library based. In a service based multi-cloud (sometimes referred to as multi-cloud as a service, or MCaaS) there is a service that acts as a broker between the multiple clouds and the user based on their SLAs or provisioning rules (Petcu, 2013). Moreover, they handle the deployment, execution, and monitoring of the clouds. In a library based multi-cloud, a single API is utilized to access and provisioning of numerous services and resources (Petcu, 2013). Some of the most widely known libraries are jclouds, Simple-Cloud, and libcloud. Jclouds is an open source Java library that enables portability of Java applications which gives stable access to resources from different IaaS providers. Simple-Cloud is a PHP library that offers a uniform interface for storing documents and files, as well as queues and infrastructure services. Libcloud is a Python library that provides an abstraction of the differences between the programming interfaces of cloud services (Petcu, 2014). The figure 2.4 illustrates the differences between these two uses of multi-cloud.

Grozev and Buyya (2014) emphasizes the independence and the involuntary interconnection of the different cloud providers, which intersects with the forced coopetition concept (Wiener and Saunders, 2014) (this will be discussed in more detail in section 2.2.2). In a multi-cloud setup, because of legal considerations an organization could use one cloud to store sensitive data and another one for data analysis (Hong et al., 2019). Some of the reasons for using multi-cloud are optimizing costs or improve Quality of Service (QoS), avoiding vendor lock-in, dealing with request peaks, and other factors (Petcu, 2014). Of note, a *hybrid-cloud* model can be considered a subset of multi-cloud networks where a private cloud deployment model is combined with one or multiple public ones regardless if the Cloud Service Providers (CSP) are unique or not (Hong et al., 2019; Rosian et al., 2022). They are often used for cloud bursting, which refers to the usage of clouds services when the private ones are insufficient (Petcu, 2014).

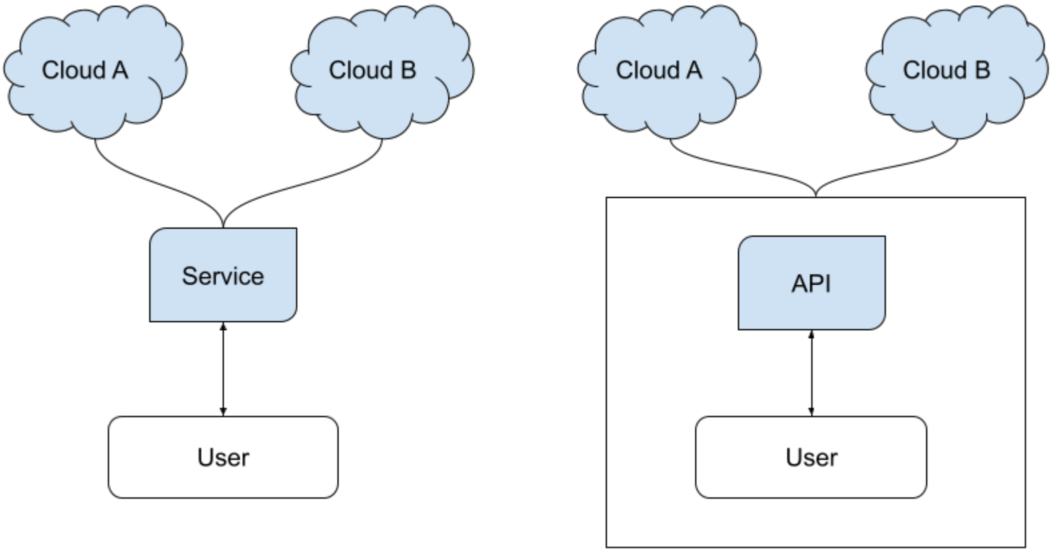

Figure 2.4: Service based and library based multi-cloud (Grozev and Buyya, 2014)

Inter-cloud

A formal definition of an inter-cloud is: "A cloud model that, for the purpose of guaranteeing service quality, such as the performance and availability of each service, allows on-demand reassignment of resources and transfer of workload through a [*sic*] interworking of cloud systems of different cloud providers based on coordination of each consumers requirements for service quality with each providers SLA and use of standard interfaces." (Grozev and Buyya, 2014, p. 371).Grozev and Buyya (2014) also note that it does not specify which of the parties that are initiating the collaboration nor if it is voluntary or not. Those factors determine whether it becomes a multi-cloud, or a federated cloud. Furthermore, (Petcu, 2014) mentions that a cloud federation or a multi-cloud becomes an inter-cloud if it includes at least one cloud broker and offers dynamic service provisioning. It is a seamless collaboration with several brokers and cloud providers to ensure that it can provide quality of service, as well as facilitating consumers to utilize various cloud providers to distribute their workloads which can help with application resilience and avoidance of vendor lock-in (Ahmed et al., 2019).

Federated cloud

In a federated cloud model there is a formal agreement between the CSPs to share spare capacity and infrastructure amongst each other (Grozev and Buyya, 2014; Petcu, 2014). The CSP voluntarily agree to share resources to ensure that they are able to support the clients data load under a single umbrella federation (Hong et al., 2019). Moreover, it gives them access to various services and resources because of the increased portability of applications. Data can also be more easily migrated between the clouds because of supporting SLAs (Hong et al., 2019). Ahmed et al. (2019) also mentions traffic load balancing and being able to handle larger spikes of traffic by having cloud providers lease their unused resources. This benefits the smaller providers in a federation, as it allows to cover for their shortcomings (Hong et al., 2019; Rosian et al., 2022). Federations can be categorized depending on their level of coupling of their cloud services. It is divided into three levels: loosely, partially, or tightly coupled. Petcu (2014) explains the differences, where in a loosely coupled federation there is little control over the cloud services and limited amount of monitoring. In a partially coupled federation, there is more control and more monitoring capabilities. Lastly, in a tightly coupled one, clouds belong to the same organization with full control and monitoring.

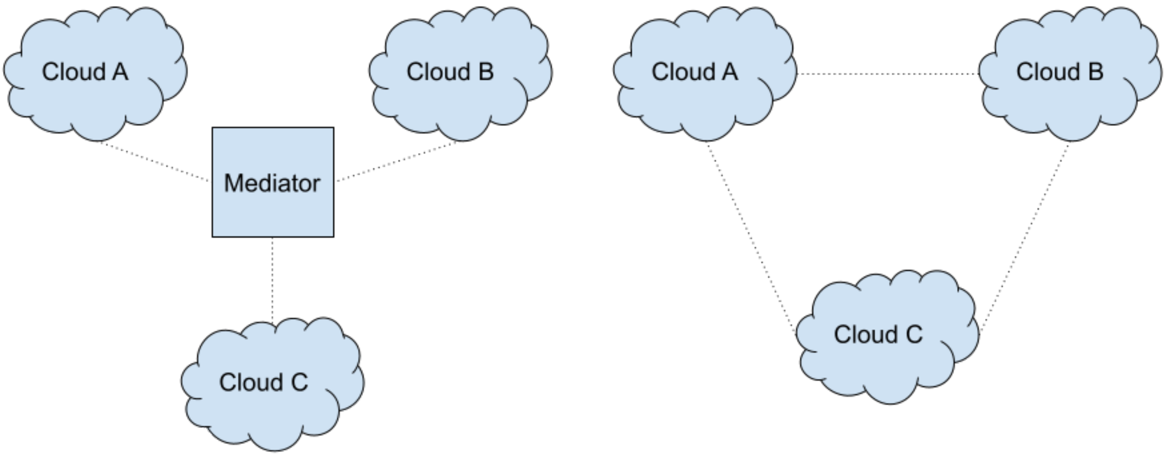

Figure 2.5: centralized cloud federation and peer-to-peer cloud federation (Grozev and Buyya, 2014)

Grozev and Buyya (2014) also classifies whether they are centralized or peer-to-peer. In a centralized federation, a central entity facilitates resource allocation, while a peer-to-peer federation communicates and negotiates directly without a mediator.

2.3.2 Multi-cloud security considerations

It is evident that security issues that concern a single-cloud model would also affect a multi-cloud model. The major difference is that a multi-cloud model consists of multiple clouds from different CSPs. With that said, there are some challenges that become more difficult to handle and some unique ones become apparent. Rosian et al. (2022) introduces some of the challenges such as an expanded attack surface, growing complexity, different security architectures, and identity and access management. Handling multiple different CSPs with differing implementations and security policies may introduce more vulnerabilities and become more prone to errors. To mitigate such vulnerabilities, Rosian et al. (2022) recommends organizations to perform a thorough risk assessment, including threat identification and risk analysis. Moreover, a multi-cloud system requires multiple logins and if the management of identity and access is inconsistent, it could introduce security risks such as illegitimate access to data. To prevent this, you could utilize a centralized security service that manages access control and use a single cloud to handle access credentials (Rosian et al., 2022). For example, one could utilize an identity and access management (IAM) solution to manage security and appoint only one of the clouds to handle username and passwords. Instead of using unique identities for every cloud, one would only need a single account to access every part of the multi-cloud. The access controls should be consistent and provide the users access to all available applications or resources in the multi-cloud using single credentials (Demchenko et al., 2017).

Afolaranmi et al. (2018) mentions that because of the increased attack surface you also need a more heightened security awareness of the components in a multi-cloud system. The amount of interfaces and endpoints are multiplied, which increases the complexity and the level of security risks and vulnerabilities. Singhal et al. (2013) identifies more security issues such as trust between CSPs, policy heterogeneity, and privacy. The customers may not have complete oversight over the multi-cloud environment and the level of security when data is moved to another cloud. Trust issues may arise as they have to entrust their data to the CSPs and hope that they are able to handle it properly. Measures must also be taken to ensure that sensitive data is not exposed in the transmission between different CSP to preserve data privacy. Moreover, policy conflicts may occur because of differing security policies among the separate CSPs. Proxies used as intermediaries were proposed by Singhal et al. (2013) to tackle these challenges. Another issue that was identified as one of the main security challenges is illicit access to virtual machines (Kritikos et al., 2015). To prevent this, they proposed an architecture that provides security with personalized spaces within the multi-cloud environment. The user can use a secure API to access these spaces as well as enforcing proper authentication and authorization.

2.3.3 Interoperability

Interoperability is the ability of different systems or components to work together seamlessly and effectively. In the context of multi-cloud environments, interoperability refers to the dexterity of handling multiple cloud computing systems to mesh together and exchange data efficiently. The newly adoption of multi-cloud systems are becoming increasingly popular due to the benefits it offers, such as increased flexibility, availability, and reliability. However, achieving interoperability between different clouds can be challenging due to differences in technology, architecture, and standards between all the CSP's services. This issue can be connected to the CIA-triad, as interoperability targets the availability section. Additionally, interoperability enables workload migration between clouds, which all are essential for disaster recovery, load balancing, and cost optimization.

Ranjan (2014) addressed three issues related to interoperability, and highlighted that these challenges may have a shortage of solutions due to lack of standardization among CSPs. Firstly, virtualization technology which allows providers to maximize physical resources, permitting multiple instances of virtual cloud resources to perform simultaneously (Ranjan, 2014). Additionally, OpenStack have been recommended by the likes of HP and Rackspace as virtualization technology. This is to solve public to private cloud interoperability issues. Nonetheless, it seems like the biggest cloud vendors will not adopt OpenStack. The second point he further addresses are the non-standardized description of the services provided by CSPs. As there are thousands of services the biggest vendors offer. As a company which tries to decide between which services fit their organization the best, it can be a tedious task to encrypt each service. This greatly reduces the visibility and control of each service, as further Service level agreements (SLA) are different and non-standardized. An interesting approach to enhance the resilience is to set up applications between multiple public -and private IaaS providers. As these usually have APIs which are not contemplated for multi-cloud interoperability. To fix this heterogeneities in APIs, it requires standardization between layers of the cloud stack. One development theory to tackle this have been by implementing a singular API that reports APIs related to multiple clouds such as services provided by Amazon (AWS EC2). The research further are to develop interoperable orchestration program modules that operate well with more vendors (Ranjan, 2014).

Ramalingam and Mohan (2021) also addresses the lack of standardization as interoperability issues of the service brokering level, semantic level and API level. As an illustration he presented a Service brokering framework, which presents the service broker and the interaction among the cloud provider and user. As there have been introduced more APIs that are available for migration and collaboration between services amidst CSPs, the standardization still falls behind. Ramalingam and Mohan (2021) sheds a light on the issues targeting semantic cloud interoperability and visibility in a multi-cloud context.

Elliott et al. (2018) also identified the interoperability issue, but focused on the use of containers. Further, he presents a container management that can migrate containers between all hosts (private, public, or both) via an interface which provides a variety of nodes, which the containers run on. This type of setup is being called cloud agnostic, which in turn means that services migrate flawlessly between the cloud platforms without disruption. Toosi et al.

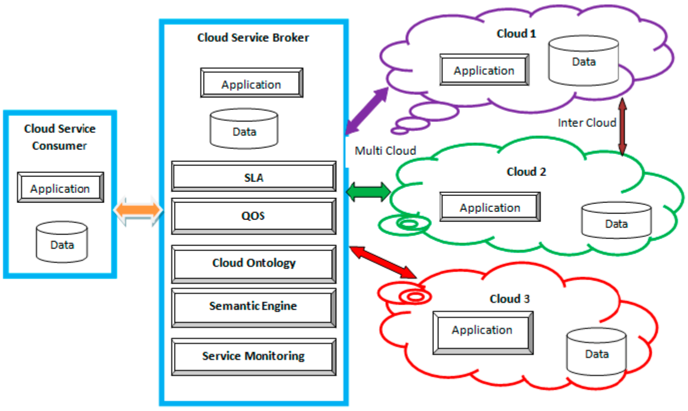

Figure 2.6: Service brokering framework

(2014) identifies the key challenges that must be addressed to achieve interoperability in multi-cloud environments. These challenges include heterogeneity, security, data management, and integration, among others. Paladi et al. (2018) propose a secure orchestration framework that enables the deployment of cloud services across different clouds while ensuring the confidentiality, integrity, and availability of the data. Finally, Ferry et al. (2013) propose a framework that utilizes models to automate the provisioning, deployment, monitoring, and adaptation of cloud services across different clouds.

Overall, the interoperability paradigm in a multi-cloud environment is a complex and multifaceted challenge that requires a combination of solutions, that could be for example standardization, semantic representation, container technology, security services, and model-driven approaches. The different approaches proposed by these articles provide a range of perspectives and potential solutions to address the interoperability challenge in multi-cloud. Although it is worth to mention CSPs commitment to allow standardization and even forced coopetition to exist.

2.4 Information security governance

Business information is an important asset for organizations and appropriate effort must be taken to protect such assets (Posthumus and R. Von Solms, 2004; R. Von Solms and von Solms, 2006). Business information is information that is of value or significance to the organization and supports its business operations (Posthumus and R. Von Solms, 2004). Technology and systems makes use of information to store, transmit, or process it to gain a business advantage (Posthumus and R. Von Solms, 2004; R. Von Solms, Thomson, et al., 2011). Because information is so valuable to the organization, it is the responsibility of the board of directors to ensure that it is protected (R. Von Solms and von Solms, 2006). Information security governance describes the process of how information security is addressed at an executive level.

Information security governance is a part of corporate governance which consists of policies and internal controls to manage organizations (R. Von Solms and von Solms, 2006). The board should provide strategic guidance for how they should operate, and further translate this into policies, standards, and procedures (R. Von Solms and von Solms, 2006). Furthermore, they mention that the board must also control the organization by ensuring that they comply with all applicable laws and regulations, as well as the aforementioned policies, standards, and procedures. This can be understood as the Direct-Control cycle, which is a core principle for all types of governance (R. Von Solms and von Solms, 2006). Directing refers to a process of communicating what is to be expected or accomplished, which can be in the form of policies (R. Von Solms, Thomson, et al., 2011). Conversely, controlling is the process to ascertain whether the policies have been complied with.

2.4.1 Direct-Control cycle

The figure 2.7 from R. Von Solms, Thomson, et al. (2011), based on R. Von Solms and von Solms (2006)'s model, describes the direct-control cycle in regards to policies. It covers the three levels of management: Strategic, tactical, and operational. Notice how it expands traversing the different levels, highlighting how the policies become more and more detailed the further down you go as the body expands on the lower levels (illustrated by the arrow on the left). It also highlights how the policies are all aligned with directives from the top of the model with no interruption in any levels. In the same vein, the compliance control (illustrated by the arrow on the right) results in less detailed reports the further up it goes. This is explained in more details below.

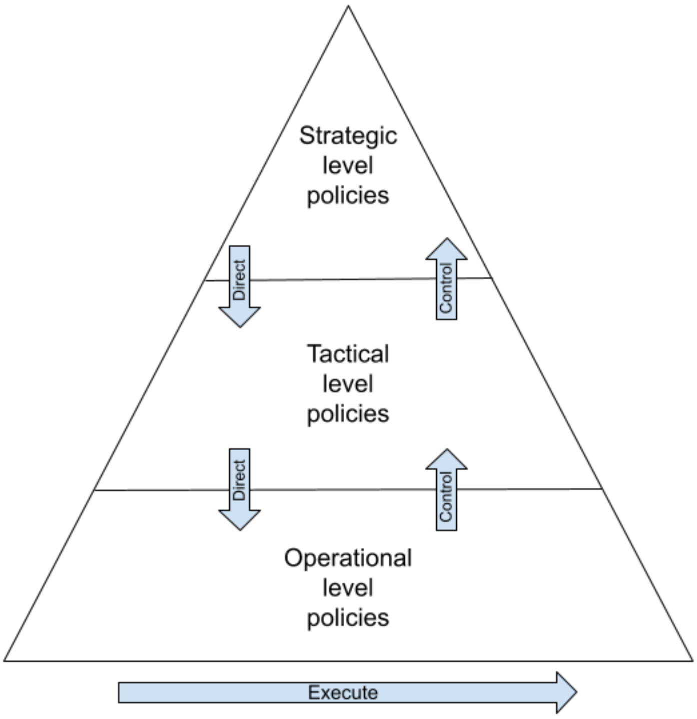

Figure 2.7: Information security policy architecture (R. Von Solms, Thomson, et al., 2011)

Direct

The 'direct' action covers all three levels. R. Von Solms, Thomson, et al. (2011) and R. Von Solms and von Solms (2006) discusses the form that it takes on the different levels. On the *strategic level*, the board must indicate the importance of the information assets and that they are a part of the strategic vision of the company. The directives they create should take into account external factors such as legal and regulatory measures, as well as internal factors like the strategic vision, the role of IT, and alignment with the company strategy, etc (R. Von Solms and von Solms, 2006). The resulting directives usually turns into a general security policy or a high level information security policy which R. Von Solms, Thomson, et al. (2011) refers to as strategic level policies. This becomes input for the next level of management (R. Von Solms and von Solms, 2006). On the *tactical level*, the directives from the previous management level turn into relevant information security policies, procedures, and standards. These are somewhat more detailed than the directives, but alignment with them is important as they also become input for the next level of management. At the *operational level*, the previous policies, standards, and guidelines are then translated into lower level policies (R. Von Solms, Thomson, et al., 2011). They reflect the operating procedures and form the basis of execution of the directives on the lowest level (R. Von Solms and von Solms, 2006).

Control

To control properly, some form of measurability must be incorporated into all directives, policies, standards, and procedures (R. Von Solms and von Solms, 2006). Any statement that can not be measured in some form should not appear in a directive or policy should it be necessary to monitor it. In the same way, 'control' also covers the three levels of management starting from the bottom. On the *operational level*, data is extracted from various entities either electronically (log files of operating systems, databases, firewalls, etc) or from analog sources such as interviews, questionnaires, inspections etc. On the *tactical level*, the measurement data from the operational level is compiled to measure against relevant policies, standards, and procedures. Furthermore, the measurement data is then aggregated to measure against the requirements of top management directives (R. Von Solms, Thomson, et al., 2011). The resulting reports indicate the levels of compliance and conformance. On the *strategic level*, the aforementioned reports are presented and should represent the risk situation in the organization (R. Von Solms and von Solms, 2006).

The gap

R. Von Solms, Thomson, et al. (2011) notes that operational level policies are usually not documented (as they are largely targeted to technical personnel) and normally takes a bottom-up approach where the technical staff would dictate security configurations and settings to then present them as policy recommendations to management, resulting in misalignment with the directives from top management. This is illustrated with the figure 2.8 below. They further categorize these policies into two types: access control, and computer networking. It is important to ensure that the policies are aligned with tactical and strategic level policies for controlling purposes.

2.5 Information security policies

The information security policy (ISP) is in essence a direction-giving document for an organizations information security (Höne and Eloff, 2002). It indicates commitment from management in their support of the organization's security, as well as the role it plays in achieving its vision and mission. Furthermore, the reason it is documented is to clarify the need for information security and its concepts to all relevant stakeholders. Security policies are important as they can provide a model for the overall security program and a platform to implement secure practices in an organization (R. Von Solms and B. Von Solms, 2004). Another objective they fulfill is to provide direction and support to management regarding business requirements and relevant laws and regulations (ISO/IEC27002, 2005).

Even though it is seen as an important part of the information security strategy in organizations (Whitman, 2008), it is clear that there is a surprising lack of literature regarding ISP development (Paananen et al., 2020). Security standards like ISO20071 (ISO/IEC27001, 2013) deem ISPs as mandatory for information security management, while some organizations do not develop their own ISPs although they acknowledge the importance of them (Yeniman Yildirim et al., 2011). One reason for this could be that the standards provide little to no guidance on how to develop good policies and what makes them effective (Höne and Eloff, 2002; M. Siponen and Willison, 2009). Another factor to consider is the fact that ISP can signify many different concepts and functions. The literature review from Paananen

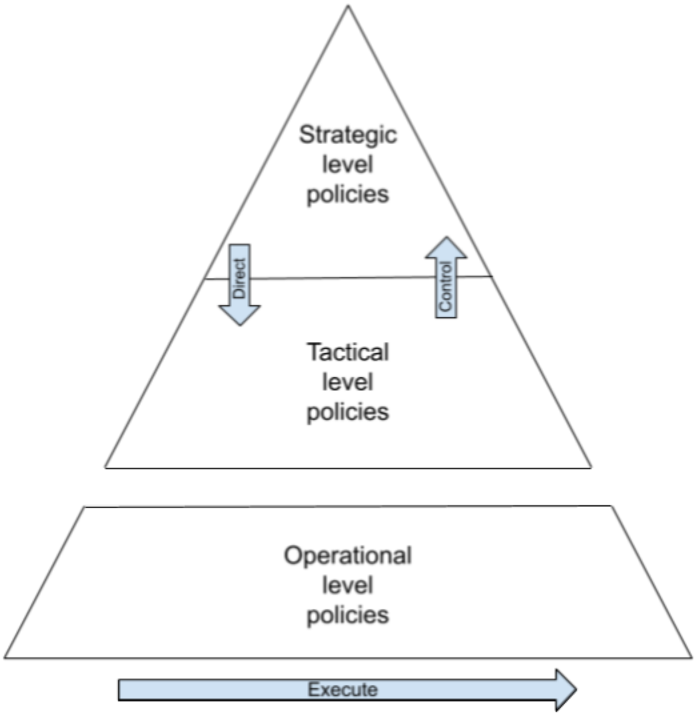

Figure 2.8: The gap between the operational level and tactical level (R. Von Solms, Thomson, et al., 2011)

et al. (2020) highlights the lack of a clearly defined definition of ISP in contemporary ISP research articles. They attempt to remedy this by enumerating relevant works on ISP and extract all the different definitions and concepts.

2.5.1 Defining ISP

ISP can be divided into technical (computer security) and non-technical (security management) (Baskerville and M. Siponen, 2002). The term "information security policy" is also commonly used in IS and information security management related textbooks and articles (Baskerville and M. Siponen, 2002). ISPs can be seen as documents that regulate the actions of people in regards to information security or expressing information security goals of the organization (Paananen et al., 2020). Another term that only covers IT assets is the information systems security policy (Balozian and Leidner, 2017). To gain an overview of the differences, Paananen et al. (2020) differentiates ISPs into three different categories. The first one is about steering the organization, how a policy can provide the organization with goals and strategies to help guide it among other things. The second one concerns the actor and the asset, which mentions how some differentiate between the people affected by the policies and the assets being protected by them. The last category is preparing for incidents, and as the name implies, it talks about how an ISP can be utilized as a countermeasure or a plan for when incidents have occurred.

Guidance

ISP is commonly represented as a statement of a desired state of security and applies terms such as "security goals", "objectives", "intentions", "strategy", and "desirable achievements" (Paananen et al., 2020). Another definition ascribe a deeper meaning to policies as a reflection of values and beliefs of the organization and its employees (Hedström et al., 2011). Many authors recommend that ISPs should complement and be aligned with the overall business goals, strategy, and objectives (Höne and Eloff, 2002; Knapp et al., 2009). Furthermore, the aim is to not only achieve security objectives such as integrity, availability, and confidentiality, but also ensuring that the organization's mission is intact despite failures or attacks against their information systems (Saleh, 2011). Understood from a policy architecture point of view, these types of policies are typically stated in the higher-level documents (Baskerville and M. Siponen, 2002).

ISPs offers guidelines for implementing information security management in organizations (Corpuz, 2011). It can be regarded as a tool for management to communicate its vision and lead the organization (R. Von Solms, Thomson, et al., 2011). Many of the instructions (directions, procedure, guidance, methods, acceptable use) are mentioned as lower-level security policies (Baskerville and M. Siponen, 2002). It can be viewed as a precondition for implementing effective deterrents and it may state penalties as well as countermeasures (Knapp et al., 2009; Rees et al., 2003). Furthermore, in case of legal disputes regarding penalties, documented policies may help to protect the organization (Tuyikeze and Pottas, 2011).

ISP can also be seen as a source of rules and protocols (Paananen et al., 2020). Some view it as a rulebook that must be followed by everyone that makes use of the organization's information (Yeniman Yildirim et al., 2011). They provide protocols and security controls to ensure the security of information systems (Ward and Smith, 2002). Klaić (2010) mentions that the policy document should also include several other layers such as standards, and guidelines for how to realize them and procedures. Metrics can be formulated to measure the effectiveness of the procedures or policies (Paananen et al., 2020). It can be viewed as a control measure by measuring compliance against the operational level policies (R. Von Solms, Thomson, et al., 2011). Paananen et al. (2020) remarks that the policy can be specifically designed in a manner where it is possible to observe its performance and link it to monetary value as a form of measurement.

Assets & actors

Baskerville and M. Siponen (2002) defines actors and assets as "security subjects" and "security objects" respectively. This is to differentiate between the actors that are affected by the policy and the assets being protected. The purpose of the policy can be to assist the individuals (or subjects) that are affected by the policy to make decisions when handling information (or objects). It is important to keep in mind that the policy is geared towards for the permitted users of the information (Yeniman Yildirim et al., 2011), which can include other external users such as business partners or third-parties (Baskerville and M. Siponen, 2002). The objects are normally defined as information systems, assets, and data (Paananen et al., 2020). Abrams and Bailey (1995) puts focus on the objects concerned in the policy by highlighting that it should specifically address information assets of the organization as well as threats to them. This is in contrast to other authors recommending that the policy should not be technology-specific (Klaić, 2010; Rees et al., 2003).

Preparing for incidents

David (2002) propose that "security is how well you adhere to your formal security policies", which can also be understood as "there is no information security without an ISP" (Paananen et al., 2020). The planning phase can be utilized to start developing security awareness in the organization (Paananen et al., 2020). The process also involves policy-planning, which promotes a better understanding of the need for security and designates acceptable security levels (Ward and Smith, 2002; Yeniman Yildirim et al., 2011). The ISP is derived from the strategic requirements for risk management (Corpuz, 2011), which is used as a tool to reduce risk to information assets. Furthermore, the ISP can also act as a recovery plan (Baskerville, Spagnoletti, et al., 2014), as well as guiding an investigation of security incidents by providing a plan of action, such as documenting the incident and containing it to limit further damage (Rees et al., 2003). The ISP document itself can be seen as a communicative object (Karlsson et al., 2017). An organization can show its efforts towards attempting to comply with regulations and standards by developing an ISP, which may also be needed in court if their actions are challenged (Whitman, 2008).

2.5.2 ISP development

As the years have passed and management have seen that ISPs directly affect the whole organization, the methods for developing ISPs have become more complex, in line with systems and organizations progression (Baskerville, 1993; Klaić, 2010). There are multiple methods of development to choose from, but finding the right fit can be a demanding task for every organization. McFadzean et al. (2007) recommended a method for for choosing the right security approach, where a business can fall into one of four categories (low to high perception of risk and whether the purpose of IT is an operational advantage). The organization's security goals should be taken into consideration, and to assess the given organization's competence to meet said goals, Saleh (2011) created an information security maturity model (ISMM). D'aubeterre et al. (2008) suggested an approach to accentuate information flows and security risks at operational level business processes with modeling languages like Secure activity resource coordination (SARC) and enriched-use case. However the information security policy architecture (ISPA) advocate that policies should firstly be assembled at the highest level of the organization, and further these strategic-level policies should be expanded or diluted to tactical and operational levels as more in depth policies (R. Von Solms, Thomson, et al., 2011).

ISP lifecycle

The policy development of ISP have been described by using various different approaches, the common proceeding is that the development process is part of a bigger lifecycle model. This is stated and accepted by numerous papers (Howard et al., 2003). To get a broader understanding Paananen et al. (2020) have made a comparison matrix (figure 2.9) from the most prominent models to represent different development models of the entire ISP lifecycle. These models highlights the differences in iterations phases of the lifecycle, which will be covered. We condensed all the models into a single ISP lifecycle which can be seen in 2.9. Ward and Smith (2002) suggested five phases in their development of an access control policy. This given method does not define input nor analysis of the raw data, but outlines the processing and outputs in depth. Further, it is not explicitly procedure for risk assessment or requirement assemblage, but are mentioned as crucial. A common misconception is to state a "general" policy development method, when one have to consider multiple characteristics and environments the organizations may have. To handle this problem Baskerville and M. Siponen (2002) have proposed an information security meta-policy where the organizations might have the need to update frequently. The main emphasis for creating policies in meta-policy is the identification and classification of policy subjects and objects. The next step, design, dictate the architecture and requirements of the policies. Ultimately the policy is implemented and tested. Baskerville and M. Siponen (2002) assert that this strategic approach would aid in defining the policy to the given organization. Howard et al. (2003) proposed the biggest model with eleven steps to execute in a security policy lifecycle. The first function, creation, additionally covers multiple separate steps; gathering data, analyzing, and creating concurrently. This models sticks out from the other models as it can be seen as granular. As multiple steps (e.g. communication, awareness, exceptions) can be considered part of the implementation function. Rees et al. (2003) describes a Policy Framework for Interpreting Risk in eCommerce Security (PFRIES) which displays thoroughly the tasks in input, development, and implementation stages. One distinct drawback with this

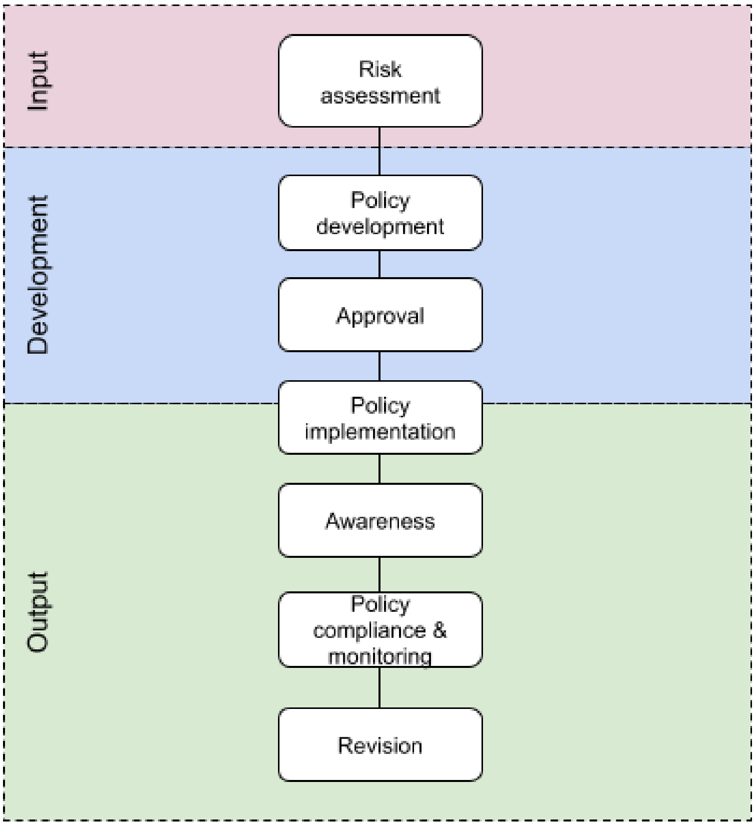

Figure 2.9: An ISP lifecycle based on Paananen et al. (2020)'s models

method is long-term preservation issues and exactly how the input should be analyzed prior to policy construction. Another criticism PFRIES have is that it does not support the adaption of policy recommendations into requirements. Antón and Earp (2001) have suggested a solution for this in the form of a Goal-based requirements-gathering (GBRAM). Knapp et al. (2009) created a more organization-level process model, which extends beyond the development team and incorporate both internal and external factors. This given model have multiple iterations within and between various phases, additionally Knapp et al. (2009) recognizes the retirement of the policy. Flowerday and Tite Tuyikeze (2016) also prescribed a broad ISP development approach, and as equal to PFRIES (Rees et al., 2003) and Knapp et al. (2009) the method has a cyclical process. In addition this method provides supplementary inputs and motivation into the whole process containing security policy (guidance and drivers), current theories, management support. After a swift introduction over the stated methods presented in figure 2.9, we can further distinguish the policy development approaches through the phases (input, development, output). Development process includes all creating or changing the content of the policy, whereas inputs and outputs include other processes that are linked to the development.

Considerations before developing

This sub-chapter will undergo respectively gathering of knowledge and analysis as separate processes from the original ISP lifecycle phases. Before the actual ISP development process can start, there must be an introductory verdict to begin with a plan to analyze the present state of the given organization and additionally security status quo (Paananen et al., 2020). Based on previous research Cram et al. (2017) discovered three aspects that impact ISP design: (1) standards & regulations; (2) fitting format; (3) internal -and external risks. Two approaches for evaluating the current state and designing the ISP which can either be a top-down approach and/or bottom-up approach (M. Niemimaa and E. Niemimaa, 2019). Trèek (2003) created a framework for both security management and policy formulation. For the policy formulation the framework recommended complying to the British standard (BS27799), which are structured as an input-process-output model. Solic et al. (2015) suggested a comparable framework, with a model that evaluates security fields into simple data. There are not only Trcek's framework that calls for the use of standards and legislation's as inputs (Burgemeestre et al., 2013; Cram et al., 2017; Horacio Ramirez Caceres and Teshigawara, 2010). Some notable examples of laws that influence ISP creation are Sarbanes-Oxley and Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR). Likewise for standards, ISO2700-series and frameworks COBIT may support the policy formulation that adheres within the law. One repercussion of fitting two sets of external requirements are often the burden on the organization (Burgemeestre et al., 2013). Contradictory to the mentioned right above, multiple authors advise not to be dependent on predefined requirements e.g. standards when plotting security (Cram et al., 2017; Dhillon and Backhouse, 2001; Hedström et al., 2011). The reason are as these approaches generally depend on revealing general risks, but can omit organizational specific threats (Baskerville, Spagnoletti, et al., 2014). All these top-down approaches needs to be migrated into an organization, which also requires bottom-up approaches. Both these two approaches can provoke constriction that needs further resolution mechanisms in the ISP development (M. Niemimaa and E. Niemimaa, 2019). From the frameworks presented in figure 2.9 Knapp et al. (2009) and Rees et al. (2003) endorse the idea that there can be a policy that can be assessed with regards to compliance, security incidents, and requirements. The frameworks also advocate a risk assessment, where potential threats and vulnerabilities are identified (Tuyikeze and Pottas, 2011). This usually includes identifying the threats, estimates value of assets, and business requirements from an IS point of view (Flowerday and Tite Tuyikeze, 2016; Rees et al., 2003; Tuyikeze and Pottas, 2011). Baskerville (1993) made a taxonomy which consisted of three generations of IS design methods: checklists, mechanistic engineering, and logical-transformational. M. T. Siponen (2005) extended these methods by adopting a more theoretical aspect against comparing the elemental assumptions of the original methods: checklists, standards, maturity criteria, risk management, and formal methods.

ISP input and output

The ISP development intrinsically is based upon using the inputs to design and define the policy as an output (Paananen et al., 2020). He further claims that the can be some lack of research surrounding of some areas, but the development phase will cover processes pertinent to designing, creating, and/or changing the contents of the policies. The development should cover the process connected to design, creation, or changing the contents of the ISP. For gathering in the necessary requirements from policy inputs and designing the policy in itself is not extensively mentioned. Although it can be useful to look at Baskerville and M. Siponen (2002), ISO/IEC27002 (2005), and R. Von Solms, Thomson, et al. (2011) to decide the various policies hierarchically. The idea of designing a given policy based upon the flow of the information pinned back to the planning phase is voiced by multiple articles, but again not much research has been done. Overall, academics and authors have been planning the policy formulation, but lacks if we look at the broader context of the lifecycle. Based on which architecture elected for the ISP, R. Von Solms, Thomson, et al. (2011) remarks that various level policies would need different development groups. As for example strategic policies will input from the same people/stakeholders that created the overall business strategy, contrary specialized IT personnel could develop the operational (lower) level policies. This could been seen as a top-down approach, which are mentioned earlier in the review, additionally have a holistic view over the whole process itself.

The next step would be to find an appropriate format for the given policy, which will affect the transparency directed to the stakeholders when implemented. Höne and Eloff (2002) advised to delineate key concept in the documentation, as the developers and readers may interpret the key concepts disparate. Here it would be appropriate to keep the text shortened and target the issue clearly. Baskerville and M. Siponen (2002) emphasis the need to do a test on the new policies. These reviews should ideally control that the policy meets the set requirements, uphold the design, and acknowledge issues in implementation (challenges, threats, etc.).

2.6 Conceptual framework

Based on the SLR, we have developed the first generic conceptual framework, illustrating the development phases of security policies for multi-cloud. The subsequent framework are based on Paananen et al. (2020) lifecycle process models (2.9) with security considerations from our previous research. As stated we wanted to combine the most relevant parts from the models, and have taken inspiration from Knapp et al. (2009) foundation, as it is more organization level focused. Where we also include internal -and external influences, which is directly targeted to various steps in said framework. Trèek (2003) explained this type of structure based on British standard (BS7799), which outlines an input-process-output model for the genesis of security policies. This first framework can be seen as a skeleton, which will be further more detailed or even remove some parts influenced by our empirical findings. However, we have made a basic foundation of the framework, and the process of the creation of these steps are given below to get a better understanding.

The input phase represented in light pink have in general consensus contained one big and crucial step. The risk assessment should be done thoroughly with potential several iterations to be done right. This assessment can be seen as the foundation block of the whole policy development process, whereas the organization should analyzing their assets and have a proper plan over the security threats given with cloud computing. Cram et al. (2017) identified three factors in this phase: standards & regulations, format, and internal -and external risks, which we have presented outside the framework.

The next phase are represented in blue, named development, which involves analyzing the previous input and design. Although various authors from the SLR claims that this phase are not properly researched yet. For the policy development there should be noted that different policy levels need different teams. When considering policy development, we decided to incorporate a top down approach, which will also require a bottom-up approach(es) (M. Niemimaa and E. Niemimaa, 2019). For example a strategic-level policy may need input from people that created the business strategy, and also down to the operational level, the IT staff may create overly technical policies. To have a holistic view over the various policy levels are beneficial, additionally to have the whole organization on board with what is planned and going to be executed. This directly transfers to the approval step, which will enforce to get consent from all parts in the organization. Most often this approval phase are from the company's executive management (Tuyikeze and Pottas, 2011). Sometimes the policy development is done after the policy is created, however reliant on the policy itself, this process can comprise sub-policies (Abrams and Bailey, 1995). This again correlates to the top-down approach, whereas a strategic-level policy can enable further down to tactical -and operational levels respectively.

The next phases are output processes, and are presented in green. A step which is described as awareness can be argued to overlap between development and output, hence displayed in gradient blended amidst the couple. This step are important as the consumer must be familiar with the new policies, which then should undergo proper training and testing. This

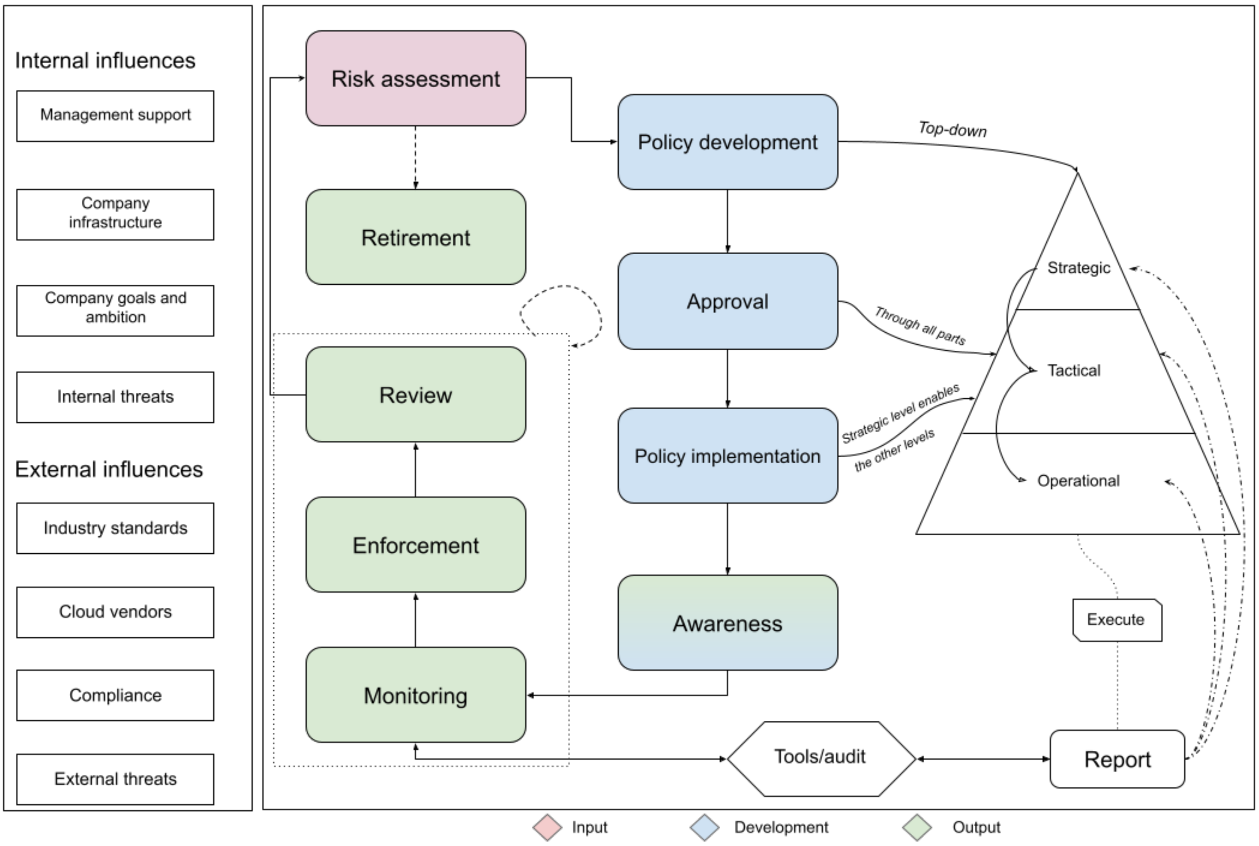

Figure 2.10: Conceptual framework

can enhance the company's long-term security culture and goals, with the implementation of a multi-cloud setup.

The monitoring step incorporates some of the components of the model from R. Von Solms, Thomson, et al. (2011) where the operational level executes relevant directives and produces information that can be monitored. Automated tools can be used to survey data from firewalls, databases, log files of operating systems, and other forms of utility, while manual audits can be performed via interviews, questionnaires, or inspections when the data cannot be sourced electronically (R. Von Solms and von Solms, 2006). The measurement data is then compiled into reports to measure compliance to strategic, tactical, and strategic policies (R. Von Solms, Thomson, et al., 2011). As a prerequisite, the security policies must be formulated in a way that enables them to be measured in some form.

What is interesting in the output phase, that it is later turns into the input phase again in a new policy development or revision process. The reason being unforeseen events may occur which will need further investigation. Monitoring potential incidents should be strong, and there could be added some KPI's to enforce this. This is a interview question we have, and will look further into. Monitoring, enforcement, and review are in a outlined box which should iterate and be done continuously, before the policy retirement.

Chapter 3

Research approach

In this chapter we will present and justify our preferred research approach, likewise we contribute arguments for how an alternate approach would be inferior for this study. The sole ambition for this exploratory research is to gain a comprehensive understanding of how multi-cloud environments affects enterprises, and how information security policies can enhance the interoperability and overall cybersecurity when dealing with more than one separate CSPs. The research design were an exploratory research as our study field have little to no prior studies. The eminent data collection were to conduct semi-structured interviews, from subjects that have a variety of experiences. To process all these findings we used an analytical tool, with also having to bear in mind the ethical considerations.

3.1 Qualitative research approach

A qualitative research approach in the context of information system research, are intended to support researchers recognize a particular phenomena[1] in context (Recker, 2021). This given approach is versatile in forms of various methods that can be implemented, most notably case study, action research, ethnography, with data sources including observation, interviews, questionnaires. Any research is based upon some fundamental philosophical assumptions, which are imperative to give some attention. When it comes to qualitative research the most prominent assumptions are tied to epistemology[2]. With inspiration from this, multiple authors and academics have proposed a three-fold classification "paradigm" of what qualitative research *can* be; positivism, interpretive, and critical (Chua, 1986; Guba and Lincoln, 1994; Orlikowski and Baroudi, 1991) as shown in the figure below. Recker (2021) highlights the differences between positivism and interpretivism and Guba and Lincoln (1994) gives an overview of critical theory in the table 3.1 below.

> *"Interpretive researchers start out with the assumption that reality (given or socially constructed) can be accessed only through social constructions such as language, consciousness, and shared meanings. Interpretive researchers generally seek to understand phenomena through the meanings that people assign to them."* (Recker, 2021, p. 116)

We find that interpretivism is the more fitting philosophical assumption to our research project as we are interested in understanding security policy development in a multi-cloud context. There is no objectively correct method for developing security policies and it is heavily dependent on the context of the organizations, which is why we need to interact with the people residing in these contexts to understand the "how" and "why". The core of interpretivism is to manipulate and understand the subjective meanings already present in

[1] "A *phenomenon* is a general result that has been observed reliably in systematic empirical research. In essence, it is an established answer to a research question" (Chiang et al., 2015)

[2] "*Epistemology* is the study or a theory of the nature and grounds of knowledge especially with reference to its limits and validity" (Merriam-Webster, n.d.)

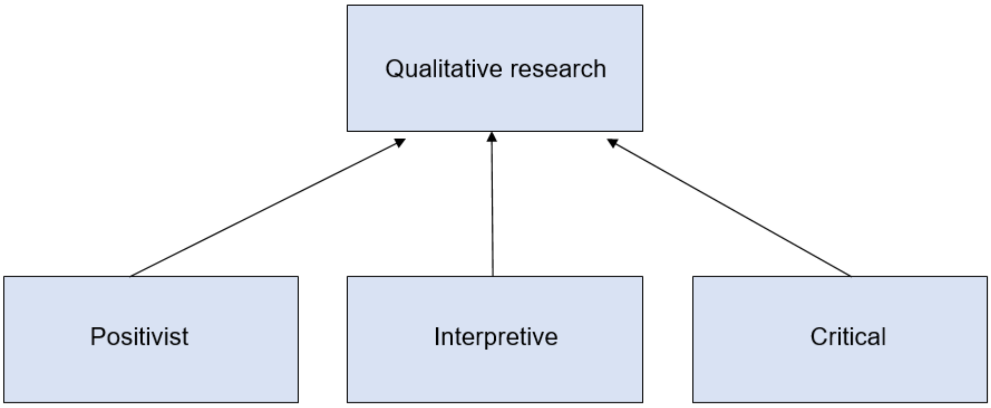

Figure 3.1: Underlying philosophical assumptions (Michael D. Myers, 1997)

Table 3.1: Table over the differences in philosophies (Guba and Lincoln, 1994; Recker, 2021)

Positivism	**Interpretive**	**Critical**
Experience is objective, testable, and independent of explanation.	Data can not be detached from theory. Data and facts are determined and shaped in light of interpretation.	Knowledge consists of a series of structural or historical insights that transforms as time passes. Transformations occur when new knowledge corrects previous instances of ignorance or misapprehensions.
Generalizations are attained from experience and are independent of the observer.	Generalizations are based on the research. Validity hinges on plausibility.	Generalizations can occur when the combination of social, cultural, economic, ethnic, and gender circumstances and values is comparable across settings.
The language of science can be exact and formal.	Languages are ambiguous and adaptive.	Reality is constructed through language.
Meaning is separated from facts.	Meanings are what constitute facts.	The surroundings influence meaning.

the social world to use as building-blocks for theory development (Goldkuhl, 2012). This is in line with our exploratory study where we will interview different subjects and attempt to interpret their subjective thoughts into meaningful data.

To motivate our choice of research approach, a table of the differences between qualitative and quantitative research is included below. Mack et al. (2005) and Recker (2021) elaborates on the different qualities of the unique approaches. Looking at the contents of the table 3.2, it becomes clear why a qualitative approach is more fitting for our thesis. Our aim is not to quantify variation, describe characteristics of a population, or extrapolate data to a broader population. We want to understand information security development in the context of multi-cloud, which is very contextual and dependent upon the experiences of the people involved. This requires a more closer look than what a quantitative approach can provide. Therefore we need to hold in-depth interviews with respondents to hear their experiences and thoughts on this subject, for us to be able to describe and explain the variations and relationships around this topic. The qualitative approach will enhance our exploratory study to ensure that we will make use of the right methods and tools to give us data that we need.

Table 3.2: Comparison between qualitative and quantitative research (Mack et al., 2005; Recker, 2021)

	Qualitative research	**Quantitative research**
Objective	To describe variation To describe and explain relationships To describe individual experiences Get a more in-depth understanding of peoples thoughts, behaviour, and motivation within different contexts	To quantify variation To predict causal relationships To derscribe characteristics of a population Extrapolate data to broader populations to get a better understanding of social phenomena
Data	Textual (from audiotapes, videotapes, and fieldnotes)	Numerical (from assigning numerical values to responses)
Data collection techniques	In-depth interviews, participant observation, focus groups	Surveys, questionnaires, structured observation
Sample size	Small case or sample	Large, representative samples
Analysis	Interpretive	Statistical
Flexibility	Some aspects of the study are flexible Participant responses can affect the interview process (e.g. follow-up questions). The study design is iterative, data collection and research questions are adjusted accordingly when needed	Study is stable from beginning to end Participant responses have no influence on the data collection process. The study design is subject to statistical assumptions and conditions

3.2 Research design

Research design is a critical component of any study and a well systematic plan involves research methodology, collection, data analysis, potential limitations and ethical dilemmas. There are many types of research design, but common to them all are intellectual reasoning which forms the core of all types of research design. As you can imagine, no study processes the same events and possibilities every time, but with a well-designed research, it enhance researchers engage in systematic patterns of intellectual reasoning to generate or test knowledge from data (Recker, 2021). Kaplan (1998) continues the subject with the aim of science is to advance human knowledge through such approaches as *extension and intension.* In this context extension indicate pursuing new fields by adopting existing knowledge in one specific field to other fields. Whereas intension invoke to gain a more exhaustive proficiency in that specific field. There are important to know the distinctions between these two terms, as extension confides in inductive reasoning and intension goes for deductive reasoning. Recker (2021) further explains the differences between the forms of reasoning;

> **Induction** is a type of reasoning that involves drawing general conclusions from specific observations or data. In research, this means starting with a set of observations or data and then using them to formulate a hypothesis or theory. Induction is often used in exploratory research, where the researcher has no prior assumptions about the topic they are studying
>
> **Deduction** is a type of reasoning that involves starting with a general principle or theory and then using it to make specific predictions about the world. In research, this means starting with a theory or hypothesis and then using it to generate specific predictions that can be tested through empirical observation. Deduction is often used

> in confirmatory research, where the researcher has a specific hypothesis or theory they want to test.
>
> **Abduction** is a type of reasoning that involves using incomplete or ambiguous observations or data to generate hypotheses or theories. In research, this means starting with a set of observations or data that don't fit with existing theories and using them to generate new hypotheses or theories. Abduction is often used in situations where there is a lack of prior knowledge or understanding of the topic being studied.

As no research process relies on these three reasoning's, we (un)intently use multiple or even all of these strategies when exploring a phenomena. Observation plays a huge part in the research process, and the observations should be reliable and precise (Recker, 2021). Well defined research designs often incorporate a blend of strategies based on induction, deduction, or abduction to fulfill a mix of exploration. Which will trigger a basic idea of a phenomenon. Rationalisation enables us to make some sense of the given problem, and lastly validation covers combines the above to rigorous testing (Oates et al., 2022).

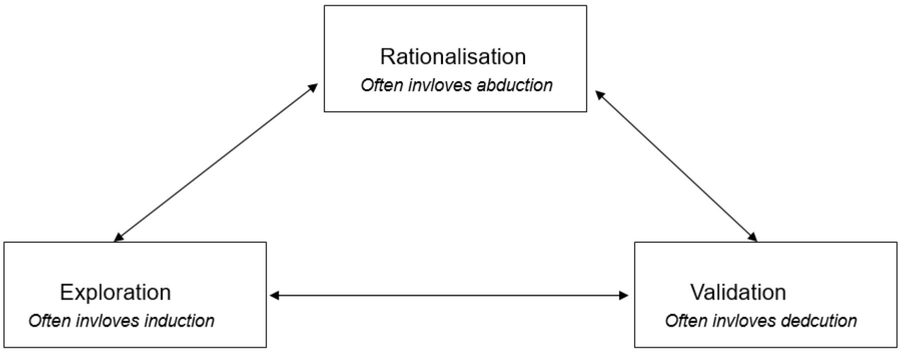

Figure 3.2: Elements of exploration, rationalisation, and validation

Based on all these terms mentioned for research design, we found an exploratory research would be most fitting given our study. This design allows us to investigate research questions that have not previously been studied enough. Hence, developing security policies in a multi-cloud context, which is as we know of, little to no exact previous research. This idea can potentially hinder some of the challenges and issues, and be a great focus for further research. As Recker (2021) stated, it is often normal to blend rationalism, exploration, and validation in one's research. Although not in a linear matter, but back and forth as illustrated in 3.2.

3.3 Data collection

As this study will go through the intricacies within a multi-cloud environment, the first step to finding an applicable subject candidate were to locate organizations that use or is familiar with cloud computing. As the research question also implies developing security policies, we would have to take a look at the subject's roles and/or previous experience. We in fact know that enterprises in Norway heavily relies on cloud computing (as mentioned in the introduction), but one rather glaring issue was to find which companies or subjects that were competent enough to fit our study, as it was no public data regarding over specific multi-cloud companies. Recker (2021) emphasis the importance of selecting the right key informants[3]. Our method were based on LinkedIn-searching, were we could filter out after organizations or role specific criteria. We needed either subjects that were familiar with the complexity of multiple CSPs or the development stages in security policies. The subjects

[3] *Key informants*, "subjects whose positions in a research setting give them specialist knowledge about other people, processes, events, or phenomena that are relevant to the research and more extensive" (Recker, 2021)

that could be appropriate would be a blend of experience from strategic -to operational levels. As we wanted a diverse pool of subjects, and also trying to avoid "elite-bias", which implies only select higher management roles. After finding suitable participants, we reached out either via message or email, additionally add a question regarding their familiarity with multi-cloud. This resulted in six willingly subjects that also fit our criteria. Hennink et al. (2020) discussed how many interviews are needed for qualitative research. Where not necessarily the number of interviews are important, but whether when we could not find any new information and resulting in saturation. In the table below we present our subject participants with their pseudonym, role, company's field, and we will elaborate on their experience further below.

Table 3.3: Subject participants

Pseudonym	**Role**	**Industry**
Region_Leader	Region Leader	IT-consultation
Service_Owner	Service Owner	IT-consultation
CTO	Chief Technology Officer & Lecturer	Delivers SaaS services
Technical_Lead	Technical Team Lead	MSP & MDR
SSA	Senior Security Architect	IT-consultation
SAC_Infra	Senior Advisor Cloud & Infrastructure	IT-consultation

As mentioned previous, we ended up with six willingly respondents with a good range of relevant roles to fulfill our research question. The variety of roles caused different opinions from a management perspective down to operational specifications. The majority of the respondents had a great experience in both IT, cloud and cybersecurity. The two main topics discussed were regarding multi-cloud challenges and developing security policies.

- **Region_Leader**'s background is primarily in Microsoft Azure, but they also have experience with Google Cloud and AWS. They participated in a multi-cloud project where they phased out an old identity service to implement an IAM to tie the authentication to a single cloud and to create only a single point they have to secure. Furthermore, they helped establish their company which provides IT-consultation services such as analysis and migration of IT infrastructure to cloud, as well as administration and optimizing hybrid or multi-cloud.

- **Service_Owner** is an IT-consultant for infrastructure and their company provides IT-consultation, focusing primarily on Azure. they do not have too much experience with multi-cloud, but they predominantly work with information security policies. They have provided one of their customers with a gap analysis and taken measure to ensure that they are compliant to the security policies they wrote. The company makes use of public and private clouds and tried to develop cloud agnostic policies to assure that they are valid independent of the cloud.

- **CTO** is a technology officer in a small startup which delivers SaaS services. They have developed an app for cybersecurity and risk management, and makes use of a multi-cloud system. The company operates nothing on-premise, most of it is on cloud. The app is hosted in Azure Kubernetes, and they use a Microsoft data center.

- **Technical_Lead** is responsible for service development within security in Azure and also leads a team that works with security and Azure. They have experience with multi-cloud solutions, citing one project with an insurance company which proved to be very complex as they need to be compliant with various laws and regulation in that type of industry. Their current company works as a Manage Service Provider (MSP), which delivers management services on top of Microsoft cloud services. They also provide also a "light" version of Managed Detection and Response (MDR), but they are not a full on SOC.

- **SSA** works as an IT-consultant in an architect group with competence in security. They have had experiences with multi-cloud systems, mentioning a project in the health sector with a sovereign cloud, which entailed a lot of compliance. They had to develop an architecture, strategy, and information security policies (strategic and technical). The sovereign cloud was hosted on a smaller Norwegian provider, and utilized the flexibility of public clouds in their asynchronous solution.
- **SAC_Infra** is the CEO of their company which provides IT-consultation. They have had experiences with multi-cloud projects before and is currently working on one.

As we decided to go for a exploratory research, conducting qualitative interviews were the most natural data collection method. Qualitative data refers to non-numeric data as e.g. words, images, and symbols generally gathered in interviews, focus groups, and company reports. The apparent data collection technique for our study is doing interviews, which is also have become the most dominant collection method (Michael D Myers and Newman, 2007). When conducting a qualitative interview researchers have to contemplate what type of interview will fit the given study. Fontana and Frey (2000) depicts these types as the following;

- Structured: A predetermined script applicable for every participant. This leaves the interview no room for improvisation, and this type is more conducive for surveys.
- Unstructured: Contrary to the structured type, an unstructured interview will not have any rigid arrangement. There will be some guided questions or themes, but researches will allow participants to speak freely over what they find relevant in the interview.
- Semi-structured: This type is more or less a hybrid between the two mentioned above. Whereas there are a interview guide, but researches will empower to ask follow-up questions. This benefits discussions around the given topic(s) or other topics that occurs.

3.3.1 Qualitative interview

We ended up with choosing a semi-structured interview (SSI) format, as it would give us a more exploratory and dynamic answers. These exploratory interviews are utilized for defining the research questions and introduce new theoretical concepts (Recker, 2021). There is a handful of aspects to take into consideration when planning, structuring, and conducting the interview guide (Appendix B). Goffman (1959) developed a theory that could be used in any social setting, the dramaturgical model. Where the interview could be seen as a "drama", where the actors (interviewers and subjects) are performing using a script. While the act, the actor's performance are studied. He defines a performance as “all the activity of a given participant on a given occasion which serves to influence in any way any of the other participants” (Goffman, 1959, p. 26). As we will continue with a semi-structured interview, some of the interview must be scripted beforehand. Some key aspects of the interview have to be written before, like the opening. Where we introduce our self, and the candidate can also feel more safe. The next are to properly explain our problem statement, to give the subject a broader understanding over what we are looking for. The last selection were to prepare some key questions. We divided the interview in two categories, multi-cloud and security policy development. As we wanted to firstly gain more understanding over how multi-cloud works in practice, and how organizations actually develop security policies. The questions should be brief and open, so it is distinguishable from quantitative questions (Kvale, 2012). There are a variation of questions to be asked, that can be used in the interview, as illustrated in the table below. Michael D Myers and Newman (2007) presented guidelines based on Goffman's model, which contains seven steps:

Table 3.4: Type of questions

	Neutral	Leading	Indirect	Secondary	Open
Example	What are your initial thoughts of...?	This framework should solve the problem, doesn't it?	Do you know whether organizations...?	Please elaborate more regarding...?	Why do you think organizations implement a multi-cloud system?
Annotations	Gives the subjects more choices	May lead to bias	If we want to ask any "touching" subjects	Actively listening to get more out of the subject, usually a following-up question	Encourages the subject to speak candidly

1. Situating the researcher as an actor. As the data from the interview can be seen as idiographic, we should locate ourself in the interviewee's shoes. Some of the introductory questions could be: "What role do you provide in the organizations?"

2. Minimize social dissonance. Therefore decrease anything that can make the subject feel uncomfortable. First impressions, suited appropriately, and using an acceptable jargon.

3. Represent various voices. As we are going to interview a variety of people, and are not trying to force anything (elite-bias)

4. Everyone is an interpreter. This emphasis the subjects are interpreters of their worlds, as we can be to theirs

5. Use mirroring in questions and answers. This mirroring-method involves to use the subjects words or phrases. Our role in the interview are to listen, encourage, and control the conversation

6. Flexibility. As an Semi structured interview (SSI) have an incomplete script, there are need for flexibility. We should be aware of various situations and reactions from the subjects

7. Confidentiality of disclosures. As we are going to record and then later transcribe, it is crucial to provide the video securely. Additionally, we are going to anonymize any name and organizations mentioned in the interview, and it is stored in One Drive at the university's network.

This model allowed us to approach the whole interview with a different vision, and made us more aware of how to conduct ourselves and the respondents. Further, some of these techniques prevented a few challenges like elite-bias. It was important for us that the interviewee felt comfortable during the interview, for optimizing the answers and opinions. Therefore, we started with a quick introduction round, followed up by some straightforward questions like: "What is your role and tasks?". As the interview went on, we utilized follow-up questions as it is an SSI. This were used to get more clarification of a topic, squeezing out every potential relevant information.

3.4 Limitations and challenges

There are many possible difficulties and problems that might occur when using a qualitative interview approach. Michael D Myers and Newman (2007) has assembled some key points in regards to what types of issues and concerns that are present and should be cognizant of:

- *Artificiality of the interview* - A qualitative interview involves questioning complete strangers to form opinions and share knowledge under time pressure.
- *Lack of trust* - Since we are a complete stranger to them, the interviewee may have some concerns to how much the interviewer can be trusted. This may result in the interviewee withholding information that they consider to be "sensitive". The result of this is an incomplete data gathering process.
- *Lack of time* - The limited amount of time we have to conduct an interview may mean that the data gathering is incomplete. This may also create the opposite problem, where the participants form opinions due to time pressure where initially they might hot have held these opinions strongly.
- *Elite bias* - It may be the case that researchers only hold interviews with high-ranking employees and may lose sight of the broader picture. This introduces bias into the research. Information gathered from high-status informants is usually taken more into consideration, while information from the lower-status ones are on the opposite end.
- *Constructing knowledge* - Interviewers are not only gathering data, they are also actively constructing knowledge. In responding to the interviewer, the subjects attempts to construct their stories in a logical and consistent manner and reflects on issues they might not have considered before. The interviewers then have to make use of their reflection to add on to previous existing knowledge.
- *Ambiguity of language* - The meaning of our words is not always clear-cut and the interviewee may not fully understand the questions we ask. This can cause the subject to misconstrue the question and answer in a way that might not be of any use to the project. Words can be ambiguous and carefully crafting questions is an important, but challenging task for the interviewer.
- *Interviews can go wrong* - Interviews can simply go wrong where the interviewer offends or unintentionally insults the interviewee, resulting in the interview being canceled altogether.

When correctly utilized, the qualitative interview is a powerful tool for gathering data. However, Michael D Myers and Newman (2007) encourages researchers to be more aware of the potential problems and pitfalls when it is used. We tried to be cognizant of these issues during the whole process of selecting interview objects, creating the interview guide, and during the interview itself. During the selection process, we tried to choose people based on whether they had experience with multi-cloud and/or security policy development without any regard for their position in the organization. Although the resulting participants were on the high-ranking end of the spectrum, they were in different positions and were able to provide us with their unique experiences and opinions on the subject matter. Including a few people that are not leaders or owners would enrich our study with more viewpoints and experiences, but was not an option due to time constraints and the lack of available interview subjects.

One of the main challenges of this approach presented itself during the subject selection process. We had no method of identifying whether or not an organization used a multi-cloud system (or just a single cloud for that matter). We ended up looking for users on

LinkedIn with any position related to cloud. This was essentially a shot in the dark and we had to specify in the mail if they had experience or used a multi-cloud system. Luckily, there were eventually six people that responded and was able to participate with relevant knowledge to share.

3.5 Data analysis

In qualitative data analysis the purpose is to organize and process the data to form an understanding of the phenomenon. The data we analyzed came from the transcription of the interviews we held and we utilized the software NVivo to code it. Coding is arguably the most commonly used method for analyzing and compressing the data to more relevant information. We coded all the interviews together to ensure that all relevant data was extracted and properly categorized. It was classified into different categories which helped when we were comparing and presenting the findings. After the first interview was coded, we developed an understanding of how the findings could be categorized to eventually confirm or contradict the findings to existing theory presented in the background section. Since the interviews were held in Norwegian, we had to translate them into English with utmost caution in an attempt to retain their original meaning without misconstruing them or misrepresent them in any way.

One crucial phase of the data analysis in qualitative research is the huge amount of data to be investigated. Where one has no correlation (yet) between the data and how it is relevant to the final outcome, because qualitative research asserts complexity, diversity, richness (Recker, 2021). A figure 3.3 made by Miles and Huberman (1994) illustrates three main stages in data analysis, where all stages are attached with the data collection:

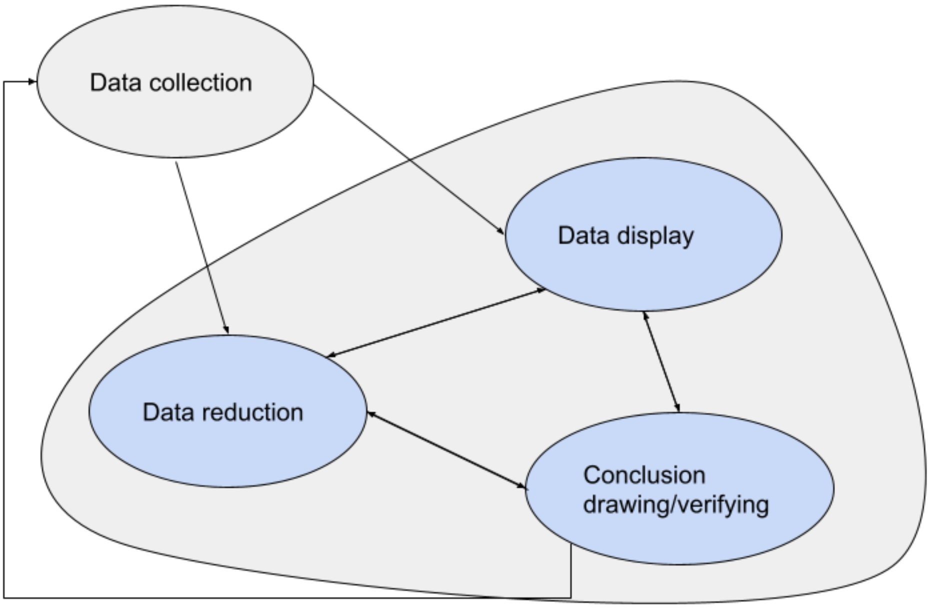

Figure 3.3: Qualitative data analysis (Miles and Huberman, 1994)

- Data reduction: This is the process to reduce and organize, where in our case we have a huge transcript (qualitative data), this was done with coding. Further irrelevant information will be scrapped, although researchers should have access to this information, as re-examining could happen.

- Data display: After the data is organized, researchers have to display the findings in a clear manner. This could be in forms of tables, diagrams, graphs, charts, etc. We have displayed some of the data as quotes.
- Conclusion-drawing and verification: This last phase is the process of how we can validate the data gathered. The most common and easy methods are probably cross-reference and checking previous studies, which is what we have done.

3.6 Ethical considerations

As we are going to collect data in the form of interviews, it is subject to ethical considerations. This is to maintain the security and confidentiality of the subject, although we did not gather in a lot of sensitive data, we had some distinguishable information: name, roles, responsibilities, processes, etc., which must be taken action to. The interview selection were voluntary participation by human subjects, meaning they could freely participate or not. We were obligated to apply and get approval from The Norwegian Center for Research Data (NSD) before conducting our interviews. This enclosed among other things, topics, subjects rights, purpose, and how the data will be secured and stored. All interviews and transcripts were stored on a encrypted cloud controlled by University of Agder, and the subject could at any time terminate the interview or see what data was collected from them.

Chapter 4

Findings

In this chapter we will present our empirical findings based on the six interviews conducted from people in various positions representing different sectors. We will present the findings in a relatively chronological order stemming from the interview guide, which were divided into two separate sections of topics, being multi-cloud and security policy development. This originates from our research question: 'How to develop information security policies in a multi-cloud environment with considerations of the unique challenges it offers?' This will also be compared to what our conceptual framework suggests, to further find any similarities or contradictions for making an improved framework as the study progresses. Some of the empirical findings that were found were the multi-cloud use in Norwegian companies, whereas both positive and negative perspectives were present. Clearly some of the issues are related to the managerial part, as the planning phase should be emphasized even more, in addition to having the right competence. The use of tools or additional services by CSPs should be utilized to optimize a multi-cloud setup. From the policy development part, we noticed a great impression to anchor through all parts of the organization. Additionally, the managerial approach top-down have been used to develop efficient policies by the companies we interviewed. Lastly, reviewing of security policies was discussed. We will elaborate further on these topics under.

4.1 Multi-cloud

Firstly we wanted to comprehend over the subjects initial thoughts regarding the use of multiple CSPs, to get an overview over the situation in today's landscape. This would enhance our research question to specifically know which threats organizations face when dealing with multi-cloud and its intricacies. To further create policies based on these challenges conferred. The subjects presented both upsides and negative effects multi-cloud can create. Some of the selling points of the whole multi-cloud trend is the selection of using each CSP's best services, creating great availability for companies. Although *SAC_ Infra* warns that multi-cloud is not necessarily trending in Norwegian companies based on the side effect like: interoperability issues, that can also make it more difficult to keep track of everything (visibility), how reliant companies have to be on CSPs, and of course the extreme complexity this can endure. Lastly, Microsoft is being mentioned as the most popular and used vendor for Norwegian consumers.

The general consensus were positive regarding the new wave of technology and could see the convenience for organizations, but the entirety of the respondents affirmed that security is a glaring issue as things stand today. One of the main selling points a multi-cloud offers is to utilize the best services from each CSP. To which both the *Service_ Owner* and *SAC_ Infra* stated:

> *"If we are looking at the availability-part, there is a huge benefit to distribute on multiple specialized platforms, and not have everything in one basket."*

The availability is mentioned by other respondents, and *Region_ Leader* claims this is a reason why organizations migrate over to multi-cloud:

> *"It is easy to start right away, and to get a competitive advantage straight away. Before we had to order equipment, hardware, long delivery time, etc. But today it is only a few clicks away. Which can absolutely be seen as a huge improvement, but also be a little bit dangerous, if not planned right."*

After we introduced the problem statement, and claimed that multi-cloud is trending, *SAC_ Infra* remarked that this is not necessarily true, from his perspective while having experience from working as a consultant:

> *"I disagree with your statement that multi-cloud is trending. From my point of view it is in a downward sloping curve. We are noticing that our clients want to dimension down, and don't necessarily see the need to run 15 different applications."*

As we are into the unique challenges a multi-cloud environment opposes, we wanted to understand what organizations need to consider when using multiple CSPs contrary to a regular single cloud computing or even on-premise. From what we researched and presented in the SLR (2.1), the interoperability between the two (or more) CSPs is a huge problem, which should be addressed with imperative measures and controls. *Service_ Owner* describes this very well:

> *"The problem is that it is not connected against the main structure where we run our policies at. So this type of solution can be very complex and difficult currently."*

There is also a risk of new measures one can not keep track of. Before it was more simpler to have control over what is happening at all times. With multi-cloud or cloud computing in general this becomes more out of control as something new is always published. *Technical_ Lead* emphasizes the complexity around this, and have a great illustration over the complexity scale.

> *"To have two different CSPs in your IT environment, it isn't just that it doubles the complexity, but more or less quadruples it. This is my statement, and it becomes so much more to control and monitor for a relatively small nation as Norway. It may be hard to find good enough employees targeting every field."*

SAC_ Infra agrees on this, and claims that one of the biggest pitfall is that the visibility is the biggest issue in multi-cloud. To have an overview over what is happening to the systems at all times are an issue today, and will have to be managed properly. Another factor is the cloud providers itself, as the company in many ways need to trust the CSP to take the right precautions. This is something they have the highest incentive to maintain. If they lose the trust of the customers, they will be in huge problems. When we are touching upon cloud providers, we thought it would be insightful to find out which cloud providers are most popular in the market in both a Norwegian -and global scale. The answers were short and unanimous: Microsoft Azure. Whereas someone roughly estimated the percentage usage was around 80-90, and coined Norway as a Microsoft-country. Not only in Norway, but generally in Europe, Microsoft is the most prominent, and Amazon on an international scale. *Region_ Leader* elaborates over his experience and views:

> *"I experienced often that we missed out on defining various things in the security policies. Frequently we don't have the "traffic rules" in order, and have to come up with a plan on the way. I think that there would be a nice benefit to have some sort of guidelines or framework for the whole multi-cloud process, not only policies, and I am sure it will come with time. As for today it is so complex, technically and strategically."*

Technical_ Lead also brings up another interesting point regarding Microsoft as a cloud provider. They are seemingly looking to become the de facto standard for integration with other cloud services. Since Azure has such a huge market share, others are motivated to be compatible with their standards to ensure that they are also able to be integrated.

> *"Microsoft is trying to position themselves as a cloud provider for other cloud providers, they incorporate security services, for example - identity is important for cloud services and Microsoft's Azure has in practice become a market standard. De facto standard - everybody supports it, those that do not support it, they do not live for long - everybody has to support Azure, even organizations that are pure Google Cloud also use Azure. This has to be secured, you should make use of the tools that are available. Microsoft has some security services that also covers Amazon and Google, so they are able to monitor the security and report on Azure."*

4.1.1 Planning

While the general focus on cybersecurity has been raised, there are still some organizations that does not take the necessary precautions before implementing a multi-cloud system. This section targets the phase before developing policies and as expected a crucial step to conquer. This section covers the importance of risk assessment, were companies today can be described as in the beginner phase of this. This phase should be aligned with the companies ambitions and core, while also respecting both security and the complexity surrounding multi-cloud. This correlates well with planning what each CSP service should do or can to affect the organization, whilst also knowing that there are no one-size-fits-all solutions.

The planning stage should be carefully analyzed and cemented into the organizations core, and is a crucial phase in developing efficient security policies. *SSA* gives input around this:

> *"To be honest, not every organization does risk assessments. I've been in many public organizations, and it is less frequent than you think. One aspect of this is that Norwegian companies are in the beginner phase of risk assessments, and they even had a multi-cloud before risk assessments were a huge part. Another rationale is that this process is highly demanding, both time consuming and expensive."*

The latter part is also mentioned by *SAC_ Infra* and *Technical_ Lead.* Contrary *Region_ Leader* have a more positive and holistic view around this topic:

> *"...Whenever one should implement new cloud services, there should be done a risk assessment/analysis. Which measures can be implemented to reduce the risk of the threats we can identify? And of course these things needs to be signed that these are the risks/threats we accept. This is not necessarily something that is being followed up correctly, but it is gaining more focus. I think this stems from that these roles usually perform "paper security", and these roles are being filled up in companies, as they can see the usefulness. So this is a good trend I can see growing over the years, because it is important and these assessments are required as well."*

The planning stage should be incorporated with the company's ambition and already established culture, and create an efficient and secure environment. There is a critical question to be answered in the likes of: What you want to secure? What are the threats? What types of threats are you scared of; phishing, ransomware, data leakage, etc. *Technical_ Lead* continues this with:

> *"We see that customers today do not really have a thorough answer to these questions. Maybe they think that 'isn't it enough with anti-virus on our computers'*

> *-mentality. That is one of the reasons they hire in professional help like us, as there are few IT departments that have dedicated security teams. Usually the security responsibility is distributed to the IT leader, a network employee, etc. They are not coordinated nor well thought out."*

Another interesting point is that there is usually no security focus from the start. There are few companies that implement e.g. ISO 27000-series from the get go, more like a sidetrack after the development is finished. This correlates directly to have strong security policy established before implementing new systems. Furthermore, implementing a standard highly regarded like ISO 27001, does not translate directly into strong security. *Technical_ Lead* & *Service_ Owner* highly advocates as they implies:

> *"...if you implement policies afterwards, you will often have many breaches which is hard to rectify in the aftermath. If you are going to implement new systems and technologies, begin with it from day one. If you're going to do it afterwards you may have a lot of things in production already, you have to calculate to use a few years to correct this properly. Because there is so much to change and to transform it, because there are a lot of dependencies and internal dependencies."*

This area, as you maybe have got the feeling of, is a potential huge downfall for organizations. There is no one-size-fits-all, as every organization is unique with their own specific needs. The planning creates a critical solid base that shines through the whole process. To have a clear understanding over what every cloud is going to be used to, and find potential shared components one can use. *SSA* claims that there is no specific multi-cloud template they follow for planning, but sees what the companies goals and ambitions are, and in-line with the infrastructure.

> *"If you're going to look into it with "policy-glasses", which applications are most secure, that can be difficult to measure, as they can be roughly the same secured. But the technical implementation of the policy could be different and some of them are far more complex to implement on certain applications in other clouds. So you have to take that into consideration in a risk assessment, if we reach the conclusion that the complexity is that tremendous that it will be easy to makes mistakes in implementation of various policies."*

4.1.2 Tools

After conducting the interviews, we got enlightened regarding the use of CSPs tools or by a third-party application, that it should almost be mandatory for succeeding in multi-cloud. These additional services are offered by each CSP, which aims to help organizations with e.g. security, policies, work-loads, compliance, etc. This can relate to the research question as a service for helping in the development phase of the policies, and additional be a practical tool for consumers to handle some of the issues. The findings from this topic were that cloud vendors do not necessarily create tools that are standardized with other CSPs. The tools for helping with policies are by the respondents lacking in terms of how the technologies are presented. There could be a solution to create a tool from scratch via an API, although it can be difficult to connect every service together. Other use cases for tools are to analyze security and compliance checking.

A problem with e.g. using Microsoft Azure's additional services is that this does not necessarily support other CSPs technologies for security and policies. *SSA* opens up about this topic as the following:

> *"There are tools that are designed to help with policies. With the intent to get a better overview, but most of the tools in the market today lacks behind in terms of*

> *what is actually needed. This can cause report fails, which can occur when using such centralized tools... And some CSPs have created tools in itself, to enhance policy administration across clouds, but the challenge indeed is that this does not support every service that exists in that specific cloud. In some cases this can operate well (use one cloud and administrate policies from there and over to the other), but it may lead to a limited amount of services again."*

A further notice for trying to resolve this issue is to use Kubernetes trust, which is intended to load balance through the CSPs to achieve a high up-time. Additionally, you have to establish strong endpoints, and make clear policy instructions regarding this setup. Another solution which is in the same track as *SSA*, were suggested by *SAC_Infra*:

> *"...One can potentially build something from scratch, because the fine thing with multi-cloud and cloud in generally in fact is that it is remarkably programmable, which means you can reach them via an API. There you could build something on your own, which again functions as a multi-cloud."*

Region_Leader remarks a fine resemblance to our conceptual framework with monitoring and tools. Which he states:

> *"You have tools in cloud which often analyzes your security status. Then you have a lot of measures, and if you do this very specific, generally not on a process level, but on predefined clear policies like two-factor authentication (2FA). Further with security status, it can display: What is the status on my tenant right now, and which measures can we take to improve the security."*

These types of tools can be extremely useful for organizations, and can additionally be used for access controls, where one can determine how many accounts have access through different roles and administrative roles, and such. Another field these tools can be useful for is to be compliant to various standards for example. *Service_Owner* makes a case for using a tool called Qualis, which performs compliance performance checks. This can also be performed by traditional datacenters, but a challenge is:

> *"There are a lot of older platforms, which causes an abundance of interruptions, and it is tremendous work to be done to get this compliant. This is naturally a huge financially burden for organizations, and often it is a risk organization can tolerate, but that allows the compliance violation to be there until the solution is replaced or being upgraded. But there are tools that can enhance the visibility of compliance for organizations."*

The use and versatility for using tools in multi-cloud is indeed a great asset to take advantage of, but should be carefully planned in-line with the organization's ambition and budget. These tools can be used for numerous of aspects in the policy creation as well, and have to be considered into the updated framework.

4.1.3 Competence

An eminently accordant topic were the competence and proficiency inside the organization. What the subjects mean by this, is that one need to hire specialized members for *each* CSP, whereas in just Microsoft Azure there is over 6-700.000 services alone, which you can imagine is extremely demanding. Let alone to be familiar enough to venture out to another platform. The competence directly targets all phases of the research questions, as the ability to tackle the multi-cloud complexity and developing security policies are dependent on who is constructing these. The highlight from the competence part could be depicted as the awareness of finding the right balance of competence. It is emphasized to hire specific experts in each cloud provider, and there is also a task to make them collaborate well.

This field can correlate well into a new section under internal influences, but one can argue a case for external as well, where organizations hire in specialized consultants. This existing knowledge have been lacking, and is crucial through all phases of developing strong policies. It already starts in risk assessment, as it is dependent of how competent these people are. Developers may have excellent developing skills, but lacks in the security and drift department. *Technical_Lead* emphasizes this, but can see an upward trend regarding this. However:

> *"A threat in cloud from a security standpoint is that the majority of organizations have experimented this, usually an IT leader, IT technician or the developing department. And further, this have just slid through in production, meaning the security is as good as you can imagine from a developer."*

The security sets in many ways a damper for developer's creativity and efficiency. Another aspect of having two separate teams with unique skill sets is to have them collaborate in a timely manner with each other. *SAC_Infra* gave us an example from a previous project where the company ended up with a split solution. One team with AWS and the other with Azure, where it was a very monotonous collaboration between the two teams. Further he discuss the importance of competence in general:

> *"You do not find an employee that have cutting edge competence in more than one platform. An Azure consultant can never replace an AWS consultant. From my experience I have never seen a multi-cloud consultant deployment, it is always separated between the platforms."*

SSA discussed the cost benefit of this, as you need competence on each platform. A contradiction between the other respondents is that *SSA* claimed that the employees would have to know something for multiple platforms, or as the majority claimed, to hire in specialized for every platform. Further supplements the collaboration between the two teams:

> *"They have to communicate with each other, this translates also to make good designs between them. If they are going to use components or load balance across platforms, they have to design good connection points for each other. So that these components can speak with each other in an efficient manner." (Interoperability)*

The systems will also have to be managed, and especially manage applications inside the cloud platforms in a good way. A service may be deprecated, or will a change cause the application to break? So in essence, organizations would have to monitor double the amount to look after if your application is distributed over both platforms and is available. *SAC_Infra* ends with that the security personnel that works all down through the operational level is acknowledged with the types of threats in the various platforms. This encourages hiring people to create their own standards or policies to handle this properly. *SAC_Infra* claims that the IT personnel in Norway lacks, and to find competent enough employees is difficult.

4.2 ISP development

In the second part of the interview, we inquired about the development process of ISPs in relation to a multi-cloud system as well as the importance of security policies. We will attempt to highlight some of the challenges with information security policy development that are pronounced in a multi-cloud context. The respondents elaborated on anchoring the security policies to the top of the organization as one of the important aspects of policy development. Furthermore, the ideal development process is the top-down approach to ensure that there is a common thread apparent in all the different levels of the policy architecture.

The strategic policies dictate how the lower level policies are developed, and they serve a clear purpose and fulfills business objectives. Lastly, reviewing policies are dependent on the level they reside at e.g. the lower they are, the more frequent updates are needed. Cloud providers come with frequent updates, at the same time there are always new technologies being released which can result in needing to revise old security policies. This is especially evident in a multi-cloud system.

When developing security policies for cloud platforms, you need to know what you need to protect and what the threats are. In line with the planning section, *Technical_Lead* highlights the importance of planning and the misconception of cloud security:

> *"When you develop security policies to assist an organization, you have to ask, what are you scared of? What do you fear? - in terms of security. There are many people that has a misconception that everything in cloud is secure straight out of the box. And that is a total misconception because it is actually very unsecure since it is made to be functional from the start, not necessarily secure."*

The ease of developing policies depends on what type it is. Generic policies as *Technical_Lead* puts it, can be very easily made, but they also have to follow up on them. He further exclaims that they should take shape as lower level operational policies, or else it is only on paper:

> *"Making policies is one thing, developing these generic policies - I could do that in 10 minutes, and I could make it suitable to any Norwegian organization. 'It is important to remember the basic principles from The Norwegian National Security Authority (NSM) and such. It is very generic, but does it have a good effect if no one is there to monitor it? It has to be materialized into technical things, or else it is just a PowerPoint-drill."*

4.2.1 Anchoring

One important aspect that was mentioned multiple times from the interviews when talking about policy development was anchoring the policy to the top of the organization. In the policy development process, it is important to understand where the policies originates from and why they hold power. Anchoring them to the top means that they are based on the will and wishes of the leaders of the organization. *Region_Leader*, *Service_Owner*, *CTO*, *SAC_Infra* and *SSA* all mentioned that you need some form of anchoring or support from the top, otherwise the policies carry no weight. *SSA* puts it very simply:

> *"You have to anchor it to the highest level, otherwise it would not make sense. If there is no anchoring then it is not valid, it breaks the chain that enables you to enforce a policy. If I just waltz in somewhere and say 'we have a policy for this', but it is not anchored, so my claim is that it is not applicable."*

Just having a policy for something is not enough. Backing from high-level positions is vital for enforcement of the policies as well as getting the employees to follow them. *CTO* expresses the same sentiments:

> *"The most important thing is having the board on board. It is important because regardless of what is written in the policy, it has no value if the board does not support it. I have been in such a situation of a policy with no support. That ended up with the security department running around and wondering about it. Security is a cooperative effort. Having the board on board is step number one, and they should preferably own it, as well as forming and signing."*

This is some of the most important work that they do when it comes to developing proper security policies. They look at where the anchoring is to ensure that the policies are properly anchored to the top level of the organization. *SSA* shares their experience when developing security policies:

> *"When I assist another business with developing security policies for this, the most crucial thing I do is, I go all the way to the top and I see where the anchoring is. It should be anchored to the leaders or the board in that organization, and it can be on a very simple level, it can be something like a "stakeholder statement" which are the directives of the organization. It can be a single line that says the organization must be secured and resilient enough to withstand attacks and not risk customer data or something similar, it can be merely a few sentences."*

The interviewees have been in agreement with some of the findings from 2.1 regarding anchoring to the top. It is preferable to have a strong policy structure, starting from the top all the way to the bottom without breaking the chain, as described by R. Von Solms, Thomson, et al. (2011) with the information security policy architecture. *SSA* Describes this process very precisely:

> *"You start from the top and then you go down a level, and this could be to the information security leader which develops some policies. Then you go down another level and arrive at the operational security where the technical people operate. They develop some standards that, like mentioned earlier, describes what sort of color should the cloud be? How should it be structured? They can also develop some guidelines or instructions and send them to the operating organization. When the operating organization receives them, they can create routines for implementing these - so you get a common thread from the top and downwards, and then you anchor it all the way through. In every stage it becomes more and more specific, such as when you are at the lowest level the guidelines can plainly say 'enter here', 'push this button', 'do it like this'. Simply put, it is implementation guidelines for how you should do it."*

The aim of anchoring is to create this common thread that helps ensure that the policies are meaningful and aligned with business objectives and goals. You have to be cognizant of what your objectives are and what is important to protect in the organization. *Service_ Owner* elaborates a little more regarding this:

> *"It is important to know the objectives of what we are doing and why we want to create this policy and the organization is concurring. If I notice that we develop overly restricting policies, then they won't gain any acceptance in the organization and you have little support to keep them. There has to be good explanations and reasons for the policies in place. For example, we said that you are not allowed to store data in the US. This is based on GDPR and the Schrems II jurisdiction, so it is relatively easy to anchor it in the organization and get an understanding for. Another example, like demanding that the data must be stored outside Europe, it would be much more difficult to gain the same acceptance. You have to know what you want to achieve, you have to know why, and you need good anchoring on much of the policies all the way up."*

These policies should be clearly documented and approved by the higher level executives. Implementing security measures should not happen ad-hoc, it should fulfill a clear objective and have a purpose. This is not always the case as *Region_ Leader* elaborates on this:

> *"That has often been the challenge, as an example when we are going to try to secure a multi-cloud system, what are the guidelines and what are the policies? The reason for having a lot of them is often because there is a lack of a security*

> *policy or standpoint from the top level... A classic example: Recently, 2-factor authentication has been very popular. It's implemented everywhere, and everyone is aware of it even if they don't use it. But there is rarely a policy that clearly states that 2FA must be implemented, it just happens. These things should be approved and stamped by the top level on clear security policies such as 2FA, passwords, identity should be secured like this, this is the process to get access, etc."*

Sometimes it is not always possible to implement these security measures, whether it is because of cost or not understanding the importance, but *Region_Leader* have noticed that the tides have started to change and organizations are starting to understand that security is needed.

> *"We see organizations become more serious and understands the significance in regards to security. There has been a large focus on cybersecurity and these things in the last few years, and it definitely helps with anchoring and these processes we are talking about right now."*

In a top-down approach, the policy development starts from the top of the organization where directives and strategies are created. These are the starting point for the common thread to trickle downwards, influencing the policy development in the lower levels of the organization. The resulting policies are a reflection of the top directives and strategy of the organization, and is also a reflection of the top executives words and will. The operational level policies that specifically targets multi-cloud must also have this common thread, to be in-line with the business objectives.

> *"But the most important thing when you have a hybrid-cloud structure, is to have a good strategical anchoring on what we are actually protecting, and the best possible way to do it. In some cases, having it strictly on paper and ensuring that everyone is aware of all the policies, can be sufficient." SSA*

4.2.2 Top-down/Bottom-up

As explained by the model 2.7, ideally the operational policies are based on general policies from the tactical level which is based on the directives from the strategic level. As mentioned before, this creates a common thread and the policies fulfill specific goals or objectives of the organization. This is the ideal scenario, but in reality, operational level policies most of the time start on the bottom at the security department as *CTO* describes it:

> *"But in practice, generally it is the security department or the IT department that writes the policy and then sends it up to the leaders to ask them if it is okay and have them sign off on it. In an ideal world, what should happen is the leaders or even the board creates the initial security policy."*

Although this is the ideal, it is not necessarily always the most optimal way of developing security policies. The leaders or the board might lack the necessary knowledge or experience to determine whether or not the policies are adequate. *Region_Leader* highlights some concerns regarding this:

> *"But oftentimes - let's say I come with a recommendation. The problem that often occurs is that the decision-makers does not understand what we are actually talking about. They just have to lean on our expertise... Usually it is an IT leader that tries to bring it into another forum - maybe a leader group."*

Developing high level policies are not seen as a challenging task. Rather, it is when you go further down to the operational level it becomes difficult. When they are developing and managing security policies for clouds, it requires a great understanding of the different architectures and systems, which demands a high level of competence from the employees. *SSA* highlights these concerns:

> *"This top down policy development approach you talk about, I don't see that as challenging if you look at the top. It becomes more difficult when you get to the lower levels. It is more demanding for the people working with security at the lowest levels, they need the right competence to understand the security challenges that are specific to the different cloud platforms when developing standards or guidelines to ensure that it is utilized in a correct manner..."*

It is on the operational level where you have to understand the differences between the cloud platforms to create different guidelines or standards. The lower levels allows for more specific policies to combat specific problems or security issues.

> *"When you get down to the technical stuff on the operational level, the differences between the different cloud providers becomes more apparent and it is there you can make standards or topic specific policies to tighten loose ends where you need it on the cloud services." SSA*

You can have topic specific policies to manage different requirements for the cloud services, but this can also become a pain point to handle. Having a demand for specific technologies when new updates and technology is released at a steady pace, can turn into a governance problem for the organization. *SAC_Infra* discuss this in regards to deployment and development of applications in clouds:

> *"You need Transport Layer Security (TLS), but should it be 1.2, 1.3, what about tomorrow when 1.5 is released? For example, is it going to be deployed? How can you manage this when people that works exclusively works with the different services, network, and so on, only see what is in front of them..."*

When developing security policies, although you might want to be very specific about what sort of technology you will make use of, some of the respondents have a differing opinion. *SSA* elaborates:

> *"Of course it is about having general policy rules that are followed and this can be requirements such as the cloud provider must comply with ISO before we can use it... They have to support safe logins and the data is secured like this or in this manner. In any case, you can have very general, but good policies. It does not have to be down to the nitty-gritty details because it is oftentimes that if you demand this and this encryption, it might not be supported. It is better if you phrase it like: 'You have to support sufficient enough encryption' as an example, but this can be a matter of definition. So being a little rounded with the security policies on a high level can be a good idea, but this can exclude a lot of providers, but the most serious one will most likely comply with such things."*

Service_Owner expresses similar sentiments:

> *"...You have to think a little bit when you develop them, and you have to think about the consequences of the contents in the policies so you don't lock yourself too much. This is because it is very easy to consider tools and technology when you create policies, but it might backfire sooner or later."*

When talking about security policies specifically for a multi-cloud system, *SAC_Infra* expresses also some concerns with the administration of these types of policies:

> *"There should be something for multi-cloud combined with TLS and network requirements. That is, this is something that is shared and should always be there, but in my opinion, it is difficult to implement those types of policies unless you have tools that can manage both parts. It becomes an administration problem if you don't have it."*

Top down, or bottom up are two different approaches when referring to policy development. This is one of the challenges when developing security policies for multi-cloud because the technical staff might want to create their own policies without considerations for top directives because of the complexities apparent in a multi-cloud system, but to ensure that these policies are contributing to business strategies and objectives, a top down approach should be encouraged.

4.2.3 Review

Review is one of the last stages of the policy development life cycle in our framework. This is one of the unique challenges in a multi-cloud system, because of the frequent updates from cloud providers, or new technology being released. In these types of cases, usually a review is needed, but the frequency of them may put too much burden on the organization, leading to fewer reviews than recommended. From the interviews we came to an understanding of how long a security policy's life cycle is. This is very dependent on what level the policy is at and the size of the organization, but in general, the higher level policies are usually longer lived, while the further down you go, the life span decreases. Or in other words, the more detailed the policy is, the faster it needs to be reviewed or retired.

> *"It was between five to ten years for the revision of a policy, and that is correct. It should last long, it shouldn't be updated all the time. What we did there was to have a long deadline for the higher level policies, but the guidelines was on a two year deadline before revision, and that was too quick. In a large organization like that, it was too fast. We should've given them some more time, like three to four years for the guidelines."* CTO

Because of the quick developments that are apparent in the IT sector, security policies are also forced to change at a faster rate than before. *Region_ Leader* shares his experience:

> *"If you consider this in combination with IT-strategy, previously you could have a ten year strategy for IT. Then many went down to five years, while five years now is like a whole era for us. Even three years have started to become drawn out, but you should be able to say where you want to be in three years. Because this goes by quick, but there are a lot of things that happens where a lot of the content in the IT strategy we wrote a year ago are no longer valid because of the rapid changes"*

SSA recommends organizations to perform check-ups on their security policies even quicker in one year intervals.

> *"For most of the documents I write, I usually recommend to have them look through it at least once a year and then they can decide whether they are still valid or if they need to be updated and then you have a continuous life cycle for these documents."*

Service_ Owner goes even further and suggests updating every six months to a year.

> *"It must be done because there is constant change. Oftentimes it is something you didn't think about, or something that conflicts with other components that performs continuous updates. I think we have settled on six months to a year, and then check on the discrepancies around this period. We update the policies if we see that there is no option to change the system to avoid any compliance violations - at least on the newer systems over a longer period of time."*

As we can clearly see from the respondents, the rapid changes in tools and technologies necessitates faster life cycles for security policies, especially on the lower levels. Although there are some small differences for the duration for when you should update them, most of the respondents agree on something around a year to validate whether the policies are still reasonable. This of course requires resources and attention from the organization which might not always be an easy task.

> *"One to two years - a lot of things have happened during the first year. Then you get these huge lists with tasks to unfold. Somebody has to fix this and that which you don't have time, money, or people for. 'No, we'll wait until next year, and then we get a new report...' Security demands constant effort. It is continuous, but again, it depends on the size of the organization and the complexity inside of the environment. The challenging part is the balancing act between security and available resources." Technical_Lead*

The organization has to make the effort to update any policies that are no longer relevant. Cloud providers or other service providers will always push out updates consistently and the organizations have to make an attempt to keep up. *SAC_Infra* makes a comment on revising policies:

> *"It depends on what you mean - from the cloud provider's perspective, you have to do it because it is very fast-paced. The development goes extremely fast, but then you have the organizations that can't keep up, and third parties usually profit from delivering multi-cloud solutions so they are usually two to three weeks behind the cloud provider. Ultimately, it is up to the organization, i.e. the customer to make these changes"*

This is also dependent on the ambition of the organization and their willingness to commit to security. *Technical_Lead* notes that the organizations need to decide what level of security is sufficient for them. They might want all the current up-to-date tools and technologies, but it might not be needed for them. It is also very dependent on the available resources of the organization, as revision is only one part of a security policy's life cycle. It is completely dependent on what type of industry they reside in and what type of data they handle. A grocery store does not need the same level of security as a hospital, but if they have the resources and ambition for it, then it does not hurt to increase the security efforts and keeping them updated. *SSA* also comments that he sees organizations struggle with getting enough people involved in the process of updating policies, which ends with an unsatisfied result.

Chapter 5

Discussion

This chapter is divided into four sections, theoretical and practical implications, future work, and lastly limitations. As we aim to discover development of information security policies in multi-cloud we decided to split it into two sections: theoretical -and practical implications, to give a presentable overview over the findings. Based on our research question: 'How to develop information security policies in a multi-cloud environment with considerations of the unique challenges it offers?', we will compare the findings to find out if it is consistent with the material presented in the background or if there are any contradictions. Furthermore, practical implications will highlight what organizations can do in practice based on the findings. Here we will give out recommendations and best practices based on the most prominent findings. To finish of the chapter we wanted to highlight any future research that can be done to improve this topic even further, additionally some of the limitations we have faced throughout the thesis.

5.1 Theoretical implications

We wanted to correlate or compare the empirical findings against previous research, hence why a theoretical implications part. This will allow us to relate the findings to the theory and discuss the reasons for why it contradicts the literature. From this we found quite a few similarities as the ISP development methodology can be seen as practically the same as the research states. Although, the risk assessment is stated in the theory to be crucial, it is not performed in practice and it should be emphasized more. Multi-cloud is as stated many times a complex and huge topic, which must be carefully planned before executed. The respondents have highlighted this and shared their thoughts over what they do or should be doing. Another interesting point is the vendor lock-in problem that multi-cloud on paper should resolve. In reality the opposite could likely happen. The shared understanding over the use of a top-down approach when developing policies were consistent with the literature. The revision of the given policy correlate somewhat with the theory, although it is independent and dynamically based on the organization. As the definition of a security policy had many descriptions in the literature, the empirical findings were agreeing on a common term. Lastly, the term forced coopetition were mentioned in the literature, meaning cloud vendors may have to operate together to satisfy multi-cloud consumers.

The general consensus gathered from the interview respondents were that the Norwegian organizations follows more or less the layout derived from life cycle process models of ISP (2.9). One of our heeds into the empirical findings were how ISP development methodology translates into development in multi-cloud organizations. Whereas our conceptual framework were based on the three input phases (input, development, and output) with sections collected from the most common or fitting models. These phases were not explicitly named, but were expressed indirectly. The risk assessment step was a unified process both from the literature and findings, although in practice multiple interviewees claims this is a shortcoming for Norwegian companies, more details described later. For the development phase it is positive to see the similarities, especially the use of including multiple parts of the company with creating strategic level policies which follows down to more operational policies. One can say that this development phase should be granted with a holistic view, so that all parts in the organization have a clear overview, we will touch upon this later also.

A number of authors suggests to perform a risk assessment as the first step for security policy development (Flowerday and Tite Tuyikeze, 2016; Knapp et al., 2009; Rees et al., 2003), but surprisingly from our interview findings, most of the respondents find that many organizations do not do this. As mentioned before, the risk assessment can be seen as the foundation block for the policy development process to analyze their assets and identify risks within the cloud environment. Without a proper risk assessment, the organization would lack a comprehensible plan for the security issues which can negatively affect the security development process. A reason for this might be that organizations underestimates the process for developing security policies. *Technical_Lead* mentioned that it is a very simple task to create policies, but to ensure that they are useful and in-line with business objectives takes more effort. Furthermore, because they do not have a clear plan, the policies might end up not as effective as they should be or they might overlook important security issues that could be mitigated with policies. As *Technical_Lead* mentioned, there is a misconception that the cloud is secure straight out of the box, and therefore they might think that assessing the security of it is redundant. It could also simply be that risk assessment is a time-consuming and expensive process, and therefore the effort is deemed disproportionate when developing policies is seen as an easy task.

One of the findings from the interviews that correlate well with the literature is the growing complexity aspect of adding and integrating another cloud into the organization (Afolaranmi et al., 2018; Rosian et al., 2022). This might seem like something that is self-evident, but the question is not if it increases, it is how much does the complexity increase. As pointed out by *Technical_Lead*, it is not a linear growth, it quadruples with a single addition. We can surmise that adding further clouds would spur on a similar increase in complexity. Therefore, managing the security of a multi-cloud system becomes a difficult task because you need the competence and resources to effectively handle it, which every organization might not have. This can have an effect on the security policy development process because they do not have a clear overview of the multi-cloud and its respective security issues. The complexity of it obfuscates the problems, making it harder to create security policies to target them. The literature suggests that using multi-cloud can optimize costs, but from our findings it seems that you need to exert an enormous amount of effort, which might turn it disadvantageous and more of a money sink. At that point does the positives outweigh the negatives, or would it be better to focus on a single cloud. Those are the questions organizations have to answer when thinking about using multi-cloud

The literature indicates that multi-cloud alleviates the vendor lock-in problem because in theory, one can switch from one cloud vendor to another if they do not provide an adequate product or it fails to fulfill the needs of the organization. In reality, it is quite different. As mentioned earlier, the complexities apparent in a multi-cloud system makes it difficult to properly utilize and integrate it. To change to another provider would require more time and resources to integrate and acclimate, which might not be a realistic option, or rather it is not as easy as the literature suggests. Furthermore, as *Technical_Lead* mentioned, Microsoft is positioning itself as a cloud provider for other cloud providers. In practice, one is highly compelled to use Azure if they are interested in using a multi-cloud system, which causes the vendor lock-in problem. This could be seen as a positive result for security policy development, as there is little motivation to switch vendors because it is such a resource heavy and time consuming process. The policies might become more stable, and their lifecycles increased in this environment.

One of the main components in the conceptual framework and were emphasized both in previous research as well as the empirical findings is the importance of a top-down approach. This managerial strategy has a variety of contributions to the policy development process. From the SLR we elaborated on R. Von Solms and von Solms (2006)'s Direct-Control model (2.7), which categorized policies into three categorizations (strategic, tactical, and operational). Utilizing a top-down approach helps ensure that there is a common thread all the way down to the operational level policies, which should be based on the strategic level ones. With this, the operational policies help with monitoring for the Control part of the cycle and fulfills business objectives because they are based on the tactical level policies, which are based on the strategic ones. This is illustrated with multiple interview subjects highlighting the importance of anchoring and support from the top of the organization. Although they understand the importance of it, in reality it is not unusual that the technical people take a bottom-up approach and develops their own security policies. This is a problem because the policies developed bottom-up will most likely not be based on the strategic level policies, which breaks the chain in the cycle. Because it is demanding and complicated to manage the security of a multi-cloud, the technical staff might think that the people higher up would not understand the difficulties of creating security policies for these systems, circumventing the top-down approach. Because they have the competency, they might think they can develop the policies without them being based on the tactical level ones.

As there are no set time frame for when one must revise their policies, there are no clear cut correct answers. It is greatly dependent on the context of the organization and at what level the policy resides at. For larger organizations, *CTO* thought that policies could remain unchanged for a longer period of time. This is also dependent on the industry they reside in. If security is paramount to their business livelihood the time frame would change. In the same vein as the literature suggested, the respondents saw that the more detailed the policy is (e.g. policies defining specific technologies or processes) the quicker the lifecycle becomes. This is because at the operational level, when technology becomes deprecated or new ones are used, the policies have to be updated at the same time. In contrast, the strategy of an organization does not change at the same pace as technology, and strategic level policies will remain relatively the same for a longer period of time. A number of respondents brought up the fact that revising policies demands resources and people for the process. In a multi-cloud system, one would need to constantly monitor for any changes in technology or updates to any of the clouds that would demand revising policies. It might not be feasible for organizations to designate resources to this problem, or it might not be prioritized over other considerations. Although it might demand resources, it is important that the policies are useful to ensure that they can help with monitoring the security situation in the Direct-Control cycle. If the security policies are not displaying an accurate view of the processes or technologies at the operational level, the whole cycle becomes broken and monitoring becomes impossible. It might be an arduous task, but reviewing policies is an important part of its lifecycle, which is why it is included in our conceptual framework.

In the background section, we investigated what an ISP or security policy is defined as, and from the interviews there were some varying answers. This seemed to be heavily dependent on their position as the more technical people such as *SAC_Infra* and *Technical_Lead* underlined operational level types (technical standards or settings), while the people on the management side such as *Region_Leader* and *CTO* had a more holistic viewpoint and emphasized strategies, objectives, and roles and responsibility. This highlights the importance of involving employees from different positions in the organization in the security policy development process. They all have different viewpoints and priorities in the context of their positions within the workplace. Neglecting any of them may end up with disregarding important security issues and result in sub-par security policies. Our framework stresses the top-down approach, which is supposed to ensure the involvement of key people on the three different management levels and aligns the policies to create a common thread.

As we mentioned earlier, Microsoft is developing their own standard to enable cooperation with other clouds and because Norway is a Microsoft country, other cloud providers are in essence forced to conform to their standard in a multi-cloud system. This somewhat coincides with the forced coopetition concept that we introduced in the 2.2.2 section. Microsoft is now included with the customer in forcing the cloud providers to cooperate with each other.

5.2 Practical implications

Contrary to the theoretical implications, we now focus on what we can use the empirical findings to give practical recommendations. Firstly, the focus of having the right competence when developing and using multi-cloud systems. Stated in the theoretical implications part, risk assessment should be taken seriously and processed properly. This aligns with involving the right people in the development phase. The use of additional services like tools are almost necessary for efficient use and cost optimization. A critical security aspect is the identity, which can be resolved by having one "main" cloud. It is also worth mentioning that every organization is unique, with different ambitions and challenges. This should be taken into consideration, while also discussing what is good enough security.

After dissecting the empirical findings there was a strong indication that the internal influence 'competency' was lacking and should be addressed properly. From the SLR there were minor considerations to this field. The small section of competence based on the background were claiming that; the level of the policy is based of the level of the people who creates the policy. This in itself is indeed true and should be considered. From the interview we quickly discovered this topic should be emphasized even more. Originally, we did not consider this relevant enough to deploy directly in the conceptual framework, although the awareness step could be argued to include this. From the empirical findings we can add a new section under internal influence, and the competence will influence multiple steps in the policy development process. This expertise could be expanded to other fields not only policies obviously, but for our study regarding policy development we see this the most fitting. A point to be taken into discussion would be the difficulty to find other specialized employees to AWS or Google, as voiced numerous times by the respondents, Norway is a heavy Microsoft-based country.

Organizations should put more focus on risk assessment to ensure that the security policy development process does not overlook important security issues, and get a better understanding of the situation at hand. This is something that should be done at the start, as it is much more difficult to implement security policies in the later stages according to one of the respondents. Ignoring the risk assessment process might make eventual avoidable situations more costly than the process itself. Furthermore, it could help with the complexity problem since it will give the organization a better understanding and overview of the clouds.

A general start point is to have a more holistic view over the whole process, meaning involving all departments in policy development. This is highlighted through our top-down/bottom-up approach, and heavily commented from the empirical findings (anchoring). With this approach all parts have a say, and are involved in the process and the organizations should ensure that the top-down approach is not broken down by the technical staff taking a bottom-up approach. The strategic level policies should be generic and easily understandable which further goes down to the operational level, which involves technical aspects of the policies. Additionally, to have the board support is crucial, as it sets the tone for the rest.

As mentioned previously these tools or additional services can be utilized for multiple purposes ranging from compliance to security. As for our research question, we want to identify how these tools can be appropriate in the policy development process. It should be mentioned that based on *SSA*s statement that some of these tools lacks functionality of what is needed in today's environment. The issue with trying to establish a centralized platform for policy overview is that there might be certain services that are not supported by *X* cloud vendor. As we can see for example that Microsoft now are trying to make their services more suitable for other CSP's applications. Although, it may cause organizations to use Microsoft as their "main" CSP, which again can initiate vendor lock-in. We wanted to highlight the potential and possible usefulness of incorporating tools into policy development. We originally placed tools by the monitoring section. This correlates well with how the findings turned out. The impact of using additional services for organizing policies and/or analyzing the status of the security can be a vital addition.

In a multi-cloud system, it can be advantageous to appoint one of the clouds to handle identity. Instead of having unique username and passwords for every single cloud in a multi-cloud system, one could have one user identity that is used by a single cloud, to then be able to access the rest of them. *Region_ Leader* has done something similar before, where they had SaaS services connected to Azure, which handled the identity. Lessening the burden on users to manage numerous amounts of username and passwords may also be practical to reduce the chance of passwords leaking. Relatedly, identity is crucial for cloud security. *Technical_ Lead* would go so far as to say that anything related to identity is 80% of the security in cloud. Therefore, one should take measurements where they can to increase the security. In the policy development process, they should take extra precaution regarding identity (e.g. make one of the clouds handle identity) to ensure that there are no unauthorized access to the cloud.

A closing remark, but nevertheless an important notice is that every organization is unique with their own goals and ambitions. *SSA* highlighted this adequately, aligned with the literature regarding the fact that there are no policy development framework that is one-size-fits-all. What we can get out of this for our study is that one can have multiple recommendations, but determinedly it is independent for every organization. Hence, why we decided to add this section in internal influence. This step should be evaluated thoroughly and accordingly to existent company structure, values, goals, etc. Another critical aspect of this is what good security is for the company. As security can be complex and a never ending rabbit hole, which expands exponentially both financially and resources required. The technical security could be far more complex in certain applications/clouds, and therefore the company must evaluate if it is worth the time or resources for this. We can advise potential organizations to consider and find what is good *enough* security which is aligned with their ambitions and budget. Of course this can be a difficult task to balance, and could require to revise set policies more frequently than planned. This step should be incorporated before and/or in the planning phase for optimal effect, and lay the foundation for the remaining development process.

Another mention regarding what is good enough security can be in some cases implemented by standards (ISO, NIST, HIPAA, etc.). To solely form your policies based on these highly regarded standards could be great of course, but this does not necessarily equal good security. We recommend to look into different standards, and based on one's intended services and infrastructure, take this into considerations in the risk assessment.

5.3 Future work

Since we did not have our framework ready before conducting the interviews, we did not have the opportunity to inquire the respondents regarding the contents of it. Therefore, the next step would be to do just that, and ask interview subjects for their opinion and change it if deemed necessary. As of now the framework is purely based on theory with no input from experts from the field of policy development. The updated framework would reflect how policy development works in reality more accurately, and the last step would be to use it in practice to have it tested with empirical data. This would determine the usefulness of the framework, where further changes could be made if needed.

It could be interesting to investigate compliance issues that are unique to a multi-cloud system. For example if an organization stores data in Europe and processes it in the US, how would an organization ensure compliance in such situations. It is a complicated area with national laws intersecting with one another, which falls outside of our scope and is why we did not include compliance in our research, but it is important nonetheless.

From our literature search, we understood that development of standards and technologies to be lacking as of now. It could be interesting to take a closer look at tools further down the line to see if they can resolve the interoperability problem of multi-cloud.

An interesting thought to entertain is the opportunity for a new position such as a multi-cloud expert/consultant. Although one of the respondent was adamant about such a position ever existing because of the complexities of it, something of the sort may end up being needed in the future. Rather than being an expert that is fully knowledgeable about two different clouds, they could assist experts of the respective clouds when handling the interoperability problem.

From the interviews, we came to understand that Norway is a Microsoft country as they put it. Most organizations make use of Azure, and therefore Azure competency is more sought after when talking about clouds. If we assume that this disparity in cloud usage also represents the amount of experts in the respective clouds, we thought it could be interesting to investigate how this imbalance between the usage of clouds could influence policy development in a multi-cloud setting. You need people with the right competency when developing operational level policies, and if there are few people that understands clouds other than the largest ones (Azure, AWS, Google Cloud), would it negatively impact the adoption of a multi-cloud system?

5.4 Limitations

A minor delay of deciding what specific topic for our thesis, resulted in a shorter time frame to create the conceptual framework for the interviews. We decided to target our questions in the interview guide to tailor the conceptual framework. Ideally the framework again should be tested after inputs from the empirical findings. This would be great to solidify our framework and an aspect in hindsight would be optimal. Although considering the time left, this was not possible.

We have made an attempt to stay objective and in our selection of literature and interview subjects when developing this thesis, but as all humans, we are capable of making mistakes or overlooking things. We may have disregarded important articles or missed opportunities that would benefit our thesis. Therefore, we can not with great confidence declare that this study contains all the important theory or findings in regards to the subject matter at hand. We have made an honest attempt to give answers to questions in this study and hopefully we can add something new to the pile of knowledge that so many other scholars have done in the past.

As multi-cloud is a relatively new technology, there was not excessive previous literature studies surrounding this topic, and even less regarding policy development in the context of multi-cloud. This could either be seen as a hinder or a challenge, we chose the latter part. The general consensus over what the challenge proposed is the security situation. As one obviously has to consider two or more clouds to monitor. Based on this annotation, we figured how to develop policies that could settle this problem. No previous papers have researched this specific topic, and we ended up using ISP development methodology to see if this was applicable for our research. After conducting the interviews, we could see that the organizations implement the same development methodology as depicted in the SLR. Although it would be great to have some more research papers to back our statements even further, but we found this topic extremely relevant and as much mentioned in the future work, it is much more to discover.

One of the cornerstones for this thesis were the empirical data, and finding suitable along with willingly respondents were difficult to assemble. Firstly, identify which organizations that operates with a multi-cloud setup were basically impossible to filter out, as there were no public information regarding this. We ended up trying to recruit consultants that had some experience with our topic. Additionally, sending out e-mails to over a hundred companies, and asking directly if they have some experience fitting our study. The other criteria for the respondents were the expertise within policy development, which every cyber/cloud security employee should have at least competent proficiency in. We ended up with six respondents which we were satisfied with, but there would be indeed appreciated with more, to get more insights and different opinions.

Chapter 6

Conclusion

The aim of this study was to gain a broader understanding over the intricate challenges organizations may face when developing information security policies in a multi-cloud context, as well as some of the issues apparent in such systems. To achieve this we have conducted a literature review to base our conceptual framework. This framework have taken inspiration from ISP development process models to tailor it into our study. The framework consist of three phases and two influences (internal and external), where it follows the whole life cycle of a policy. The development phase is greatly inspired by the managerial approach coined top-down approach, which we see as most optimal for the majority of organizations as it allows a holistic view. Further, based on the empirical findings from our interviews, we also addressed these impressions and practical suggestions which could add to the conceptual framework, although no changes were made. It has been a journey full of surprises and learning regarding this huge topic, and a field that will continue to grow as time goes.
We will present our main findings to summarize our conclusion, in addition to address the research question stated for the thesis: *How to develop security policies in a multi-cloud environment with considerations of the unique challenges it offers?*

Main findings

- **Planning:** Even before implementing a multi-cloud system, organizations have to consider the business need and security factors of utilizing such systems. To enable and carry out cloud services are just a few clicks away. Are these services business critical or just a cordial technology to be utilized? The empirical findings highlights the importance of aligning the planning of a multi-cloud to be in-line with the already established infrastructure, ambitions and goals. To further expand on the planning step, a risk assessment is a prerequisite for every company. This is profoundly emphasized both by the literature and empirical findings. In practice we could uncover that Norwegian organizations do not necessarily regulate such assessments. As it could be stated that this is a fairly "new" approach of implementing technologies. However, these assessments are vital for further developing satisfactory security policies. As this can uncover potential vulnerabilities and threats, or disclose hidden dilemmas. This step directly targets the whole research question as the planning unfolds security issues, assembles the policy development process and prioritizes multi-cloud aspects.
  With that being stated, it is imperative to note that every organization is different with their own aspirations, values, struggles, etc. Although we presented a framework, this is by no means a one-size-fits-all. These considerations should always be valued and discussed how to make the best out of one's situation. An interesting statement from the interviews were regarding the policies being based on a standard. This does not necessarily translate to good security. Additionally, every organization should define

what is good enough security for their needs. If not, it can lead to wasting resources, time, and cost. Not every data is evenly important for an incident, so to identify which data should be prioritized.

- **Top-down approach:** Developing information security policies has usually two different approaches, top-down or bottom-up. Following the Direct-Control cycle, security policies should start from the top of the organization to ensure that the policies on the tactical, and operational level are based on the strategic ones. This will provide a common thread where the operational policies are based on the tactical policies, which are based on strategic policies. The result is that the operational policies will be effective in fulfilling the business objectives and be able to be monitored for the same purpose. Because of the complexities apparent in a multi-cloud system, the people working on the operational level might be inclined to develop their own security policies without concern for aligning them with the higher level ones, breaking the Direct-Control cycle. This would make monitoring the policies and their effectiveness in fulfilling the business objectives difficult because they would not be based on higher level policies, but rather it would only be concerned about satisfying the needs on the operational level. To avoid this problem, the top-down approach is preferable when developing security policies. This would also help with involving people on all the levels and ensure that the policies are properly anchored and supported from the top of the organization.

- **Competence:** Something that was not mentioned in the literature, but many of the respondents highlighted was the fact that competency is important when dealing with the complexities that are evident in a multi-cloud system. To develop security policies specifically for multi-cloud, one would need the competency to accurately understand the security issues present in each unique cloud and how to mitigate it. This can be difficult in the Norwegian context, where most organizations utilize Microsoft Azure, therefore getting people with the right competence may prove to be a challenge. To mitigate this, proper planning with risk assessment and analysis can help to give an overview and identify where security policies can help mitigate obvious security issues.

- **Use tools/additional services:** An eminent factor based from the empirical findings is the importance of taking advantage of tools or additional services provided by the CSPs. This targets the policy development and partially multi-cloud issues, but for the relevancy of the research question, we opted to focus on the development process. As presented in the conceptual framework, tools can directly aid the monitoring phase of the policy development. This includes analyzing the security, regulate compliance, and automating processes. This is especially useful in multi-cloud, as it can be difficult to get an overview over all the policies and services implemented. The empirical findings targeted the attention by valuing the additional services offered by vendors. Even some of them implying that it is a necessity to take advantage of. The versatility these third party applications can be utilized for, is highly valued. Although, we do not recommend to carelessly implement every service, but to evaluate which components fits the organizational structure to implement it via the policies. This is for cost optimization and efficient use of resources.

- **Vendor lock-in:** An interesting point that should be reflected on is one of the issues multi-cloud on paper should resolve. The vendor lock-in issue is generated by organizations getting dependent on one CSP, hence vendor lock-in. In reality multi-cloud can indeed cause this issue. This stems from the section above (tools), whereas an organization could be solely dependent on these services provided by the vendor, which in turn generates a lock-in issue again. This section focuses on the security considerations of the research question, and partially policy development, as this is a concern to be taken into consideration before implementing a multi-cloud setup.

- **Reviewing policies:** Review is one of the last stages of an information security policy's lifecycle in our conceptual framework. It may seem like a simple process to just evaluate security policies and judge whether or not they are useful or still valid after a period of time, but it is still a process that is time-consuming and requires resources and people. Organizations might not prioritize revising security policies because of this cost. There are also no clear guidelines for when one should review policies, but in general, the more detailed the policy is the quicker a review is needed. To illustrate, strategic ones detailing strategies and security goals does not have to be revised in a short timeframe, while operational ones detailing specific tools, technologies, or processes should be updated more frequently because of the rapid changes in such environments. This is especially apparent in a multi-cloud system where one must monitor multiple vendors for updates and substitutions in technology to eventually review policies affected by these changes. It becomes more difficult because of the complexity and the competence needed to maintain such a system, and its respective security policies. Although it is a demanding task, it is important to review the policies to ensure that the Direct-Control cycle is not broken. In such a situation the security policies does not accurately reflect the security situation and it becomes impossible to monitor and the policies would not bring any value to the organization. This is why it is important to review security policies and revise if needed, especially in a multi-cloud system.

To end the thesis, we wanted to give some closing thoughts regarding the whole experience and study. This exploratory study have been an extensive process with a steep learning curve from day one, in a hugely relevant and timely topic. The fact that there were, as we know of, little to no previous studies, motivated this thesis even further. We wanted to provide a conceptual framework to aid organizations that is considering the change, or already utilizing multi-cloud. There should be stated that this is by no means a guideline, but rather a starting point for further discussion and future work. This field is enormous, with endless factors that should be considered. We see this can be resolved eventually with e.g. improved standardized solutions that CSPs could provide. In addition, as it is a fairly new field, we can just hope that this could be a push in the right direction. Having the right planning strategy and security policies on board establishes a solid foundation for utilizing this complex system. This thesis have given us a strong indication for this topics situation as things stand today, and challenged us to achieve the best possible result.

Bibliography

Abrams, M., & Bailey, D. (1995). Abstraction and refinement of layered security policy. *Information Security: An Integrated Collection of Essays*, 126–136.

Afolaranmi, S. O., Ferrer, B. R., & Lastra, J. L. M. (2018). A framework for evaluating security in multi-cloud environments. *IECON 2018-44th annual conference of the IEEE industrial electronics society*, 3059–3066.

Ahmed, U., Raza, I., & Hussain, S. A. (2019). Trust evaluation in cross-cloud federation: Survey and requirement analysis. *ACM Computing Surveys (CSUR)*, *52*(1), 1–37.

Alpar, P., & Polyviou, A. (2017). Management of multi-cloud computing. *Global Sourcing of Digital Services: Micro and Macro Perspectives: 11th Global Sourcing Workshop 2017, La Thuile, Italy, February 22-25, 2017, Revised Selected Papers 11*, 124–137.

Antón, A. I., & Earp, J. B. (2001). Strategies for developing policies and requirements for secure and private electronic commerce. *E-commerce security and privacy*, 67–86.

Balozian, P., & Leidner, D. (2017). Review of is security policy compliance: Toward the building blocks of an is security theory. *SIGMIS Database*, *48*(3). https://doi.org/https://doi.org/10.1145/3130515.3130518

Bapna, R., Barua, A., Mani, D., & Mehra, A. (2010). Research commentary—cooperation, coordination, and governance in multisourcing: An agenda for analytical and empirical research. *Information Systems Research*, *21*(4), 785–795.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys (CSUR)*, *25*(4), 375–414.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics information management.*

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & management*, *51*(1), 138–151.

Burgemeestre, B., Hulstijn, J., & Tan, Y.-H. (2013). Value-based argumentation for designing and auditing security measures. *Ethics and information technology*, *15*, 153–171.

Chiang, I.-C. A., Jhangiani, R. S., & Price, P. C. (2015). Phenomena and theories. https://opentextbc.ca/researchmethods/chapter/phenomena-and-theories/

Chua, W. F. (1986). Radical developments in accounting thought. *Accounting review*, 601–632.

Corpuz, M. (2011). The enterprise information security policy as a strategic business policy within the corporate strategic plan. *Proceedings of the 15th Multi-Conference on Systemics, Cybernetics and Informatics, WMSCI 2011: Volume III*, 275–279.

Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, *26*, 605–641.

D'aubeterre, F., Singh, R., & Iyer, L. (2008). Secure activity resource coordination: Empirical evidence of enhanced security awareness in designing secure business processes. *European Journal of Information Systems*, *17*(5), 528–542.

David, J. (2002). Policy enforcement in the workplace. *Computers & Security*, *21*(6), 506–513. https://doi.org/https://doi.org/10.1016/S0167-4048(02)01006-4

Demchenko, Y., Turkmen, F., Slawik, M., & De Laat, C. (2017). Defining intercloud security framework and architecture components for multi-cloud data intensive applications. *2017 17th IEEE/ACM international symposium on cluster, cloud and grid computing (CCGRID)*, 945–952.

Dhar, S. (2012). From outsourcing to cloud computing: Evolution of it services. *Management research review*, *35*(8), 664–675.

Dhillon, G., & Backhouse, J. (2001). Current directions in is security research: Towards socio-organizational perspectives. *Information systems journal*, *11*(2), 127–153.

Elliott, D., Otero, C., Ridley, M., & Merino, X. (2018). A cloud-agnostic container orchestrator for improving interoperability. *2018 IEEE 11th international conference on cloud computing (CLOUD)*, 958–961.

Ferry, N., Rossini, A., Chauvel, F., Morin, B., & Solberg, A. (2013). Towards model-driven provisioning, deployment, monitoring, and adaptation of multi-cloud systems. *2013 IEEE Sixth International Conference on cloud computing*, 887–894.

Flexera. (2022). State of the cloud report.

Flowerday, S. V., & Tuyikeze, T. [Tite]. (2016). Information security policy development and implementation: The what, how and who. *computers & security*, *61*, 169–183.

Fontana, A., & Frey, J. H. (2000). The interview: From structured questions to negotiated text. *Handbook of qualitative research*, *2*(6), 645–672.

Goffman, E. (1959). The presentation of self in everyday life: Selections.

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European journal of information systems*, *21*, 135–146.

Grozev, N., & Buyya, R. (2014). Inter-cloud architectures and application brokering: Taxonomy and survey. *Software: Practice and Experience*, *44*(3), 369–390.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In *Handbook of qualitative research* (pp. 105–117). Sage Publications.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), 373–384. https://doi.org/https://doi.org/10.1016/j.jsis.2011.06.001

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods*. Sage.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say? *Computers & security*, *21*(5), 402–409.

Hong, J., Dreibholz, T., Schenkel, J., & Hu, J. (2019). An overview of multi-cloud computing. https://doi.org/10.1007/978-3-030-15035-8_103

Horacio Ramirez Caceres, G., & Teshigawara, Y. (2010). Security guideline tool for home users based on international standards. *Information Management & Computer Security*, *18*(2), 101–123.

Howard, P. D., et al. (2003). The security policy life cycle: Functions and responsibilities. In *Information security management handbook* (pp. 1353–1366). Auerbach Publications.

ISO/IEC27001. (2013). Information technology — security techniques — information security management systems — requirements.

ISO/IEC27002. (2005). Information technology — security techniques - code of practice for information security management.

Kaplan, R. S. (1998). Innovation action research: Creating new management theory and practice. *Journal of management accounting research*, *10*, 89.

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security*, *67*, 267–279. https://doi.org/https://doi.org/10.1016/j.cose.2016.12.012

Kitchenham & Charters. (2007). Guidelines for performing systematic literature reviews in software engineering.

Klaić, A. (2010). Overview of the state and trends in the contemporary information security policy and information security management methodologies. *The 33rd International Convention MIPRO*, 1203–1208.

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & security*, *28*(7), 493–508.

Kritikos, K., Kirkham, T., Kryza, B., & Massonet, P. (2015). Security enforcement for multi-cloud platforms–the case of paasage. *Procedia Computer Science*, *68*, 103–115.

Kvale, S. (2012). *Doing interviews*. Sage.

Lee, J.-N., Huynh, M. Q., Kwok, R. C.-W., & Pi, S.-M. (2003). It outsourcing evolution— past, present, and future. *Communications of the ACM*, *46*(5), 84–89.

Mack, N., Woodsong, C., MacQueen, K. M., & Guest, G. (2005). *Qualitative research methods*. Family Health International.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing it on information security strategy at board level. *Online Information Review*, *31*(5), 622–660.

Merriam-Webster. (n.d.). Epistemology definition and meaning.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.

Myers, M. D. [Michael D.]. (1997). Qualitative research in information systems. *MIS Quarterly*, *21*(2), 241–242. https://doi.org/10.2307/249422

Myers, M. D. [Michael D], & Newman, M. (2007). The qualitative interview in is research: Examining the craft. *Information and organization*, *17*(1), 2–26.

Niemimaa, M., & Niemimaa, E. (2019). Abductive innovations in information security policy development: An ethnographic study. *European Journal of Information Systems*, *28*(5), 566–589.

Oates, B. J., Griffiths, M., & McLean, R. (2022). *Researching information systems and computing*. Sage.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research*, *2*(1), 1–28.

Oshri, I., Dibbern, J., Kotlarsky, J., & Krancher, O. (2019). An information processing view on joint vendor performance in multi-sourcing: The role of the guardian. *Journal of Management Information Systems*, *36*(4), 1248–1283.

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, *88*, 101608.

Paladi, N., Michalas, A., & Dang, H.-V. (2018). Towards secure cloud orchestration for multi-cloud deployments. *Proceedings of the 5th Workshop on CrossCloud Infrastructures & Platforms*, 1–6.

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, *52*(2), 183–199.

Petcu, D. (2014). Consuming resources and services from multiple clouds: From terminology to cloudware support. *Journal of Grid Computing*, *12*(2), 321–345.

Petcu, D. (2013). Multi-cloud: Expectations and current approaches. *Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds*, 1–6.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & security*, *23*(8), 638–646.

Ramalingam, C., & Mohan, P. (2021). Addressing semantics standards for cloud portability and interoperability in multi cloud environment. *Symmetry*, *13*(2), 317.

Ranjan, R. (2014). The cloud interoperability challenge. *IEEE Cloud Computing*, *1*(2), 20–24.

Recker, J. (2021). *Scientific research in information systems: A beginner's guide*. Springer.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). Pfires: A policy framework for information security. *Communications of the ACM*, *46*(7), 101–106.

Rosian, M., Altendeitering, M., & Otto, B. (2022). A socio-technical analysis of challenges in managing multi-clouds.

Saleh, M. F. (2011). Information security maturity model. *International Journal of Computer Science and Security (IJCSS)*, *5*(3), 21.

Schmidt, K., & Suomi, P. D. R. (2018). It multisourcing management.

Schrama, A. (2021). *Managing multi-cloud systems: A framework for effective management and governance of multivendor cloud arrangements* (Master's thesis). Delft University of Technology.

Singhal, M., Chandrasekhar, S., Ge, T., Sandhu, R., Krishnan, R., Ahn, G.-J., & Bertino, E. (2013). Collaboration in multicloud computing environments: Framework and security issues. *Computer*, *46*(2), 76–84.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270. https://doi.org/https://doi.org/10.1016/j.im.2008.12.007

Siponen, M. T. (2005). An analysis of the traditional is security approaches: Implications for research and practice. *European Journal of Information Systems*, *14*, 303–315.

Solic, K., Ocevcic, H., & Golub, M. (2015). The information systems' security level assessment model based on an ontology and evidential reasoning approach. *Computers & security*, *55*, 100–112.

Statista. (2023). Revenue of the public cloud market in norway from 2018 to 2027.

Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Interconnected cloud computing environments: Challenges, taxonomy, and survey. *ACM Computing Surveys (CSUR)*, *47*(1), 1–47.

Trèek, D. (2003). An integral framework for information systems security management. *Computers & Security*, *22*(4), 337–360.

Tuyikeze, T., & Pottas, D. (2011). An information security policy development life cycle. *Proceedings of the South African Information Security Multi-Conference (SAISMC), Port Elizabeth, South Africa*, 165–176.

VentureBeat. (2022). Report: 69% of orgs report multicloud security configurations led to data breaches or exposures.

Von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *2011 Information Security for South Africa*, 1–6.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & security*, *23*(4), 275–279.

Von Solms, R., & von Solms, S. B. (2006). Information security governance: A model based on the direct–control cycle. *Computers & Security*, *25*(6), 408–412.

Wanden-Berghe, C., & Sanz-Valero, J. (2012). Systematic reviews in nutrition: Standardized methodology. *British journal of nutrition*, *107*(S2), S3–S7.

Ward, P., & Smith, C. L. (2002). The development of access control policies for information technology systems. *Computers & Security*, *21*(4), 356–371. https://doi.org/https://doi.org/10.1016/S0167-4048(02)00414-5

Whitman, M. E. (2008). Security policy. *POLICY, PROCESSES, AND PRACTICES*, 123.

Wiener, M., & Saunders, C. (2014). Forced coopetition in it multi-sourcing. *The Journal of Strategic Information Systems*, *23*(3), 210–225.

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of planning education and research*, *39*(1), 93–112.

Yeniman Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from turkey. *International Journal of Information Management*, *31*(4), 360–365. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2010.10.006

Appendix A

List over literature

Author(s)	Title	Database	Search string
Paananen et al. (2020)	State of the art in information security policy development	Web of science	("information security policy" AND "development" OR "methodology")
Afolaranmi et al. (2018)	A framework for evaluating security in multi-cloud environments	Scopus	("multi-cloud" OR multicloud) AND security AND framework
Singhal et al. (2013)	Collaboration in Multicloud Computing Environments: Framework and Security Issues	IEEE Xplore	("multi-cloud" OR multicloud) AND security AND framework
Petcu (2013)	Consuming resources and services from multiple clouds: from terminology to cloudware support	Scopus	("multi-cloud" OR multicloud) AND (terminology OR taxonomy)
Hong et al. (2019)	An overview of multi-cloud computing	Google Scholar	("multi-cloud" OR multicloud) AND " challenges"
Grozev and Buyya (2014)	Inter-cloud architectures and application brokering: Taxonomy and survey	Scopus	("multi-cloud" OR multicloud) AND (terminology OR taxonomy)
Posthumus and R. Von Solms (2004)	A framework for the governance of information security	Google Scholar	"information security" AND "governance"
R. Von Solms and von Solms (2006)	Information security governance: A model based on the direct–control cycle	Google Scholar	"information security" AND "governance"
R. Von Solms, Thomson, et al. (2011)	Information security governance control through comprehensive policy architectures	Google Scholar	"information security" AND "governance"
Wiener and Saunders (2014)	Forced coopetition in IT multi-sourcing	Web of science	("IT sourcing" OR "multi-sourcing")
Bapna et al. (2010)	Research commentary—cooperation, coordination, and governance in multisourcing: An agenda for analytical and empirical research	Google Scholar	("IT sourcing" OR "multi-sourcing")
Ranjan (2014)	The Cloud Interoperability Challenge	IEEE Xplore	("multi-cloud" OR multicloud) AND " challenges"

Toosi et al. (2014)	Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey	Scopus	("multi-cloud" AND " challenges")
Elliott et al. (2018)	A Cloud-Agnostic Container Orchestrator for Improving Interoperability	Google Scholar	"cloud" AND ("security" OR "interoperability")
Ramalingam and Mohan (2021)	Addressing Semantics Standards for Cloud Portability and Interoperability in Multi Cloud Environment		Snowballed
Paladi et al. (2018)	Towards Secure Cloud Orchestration for Multi-Cloud Deployments		Snowballed
Ferry et al. (2013)	Towards model-driven provisioning, deployment, monitoring, and adaptation of multi-cloud systems		Snowballed
Kritikos et al. (2015)	Security enforcement for multi-Cloud platforms–The case of PaaSage		Snowballed
Ward and Smith (2002)	The development of access control policies for information technology systems		Snowballed
Baskerville and M. Siponen (2002)	An information security meta-policy for emergent organizations		Snowballed
Rees et al. (2003)	A policy framework for information security		Snowballed
Knapp et al. (2009)	Information security policy: An organizational-level process model		Snowballed
Tuyikeze and Pottas (2011)	An information security policy development life cycle		Snowballed

Table A.1: Reviewed articles

Appendix B

Interview guide

Del 1: Generell informasjon

1. Hvilken rolle har du i bedriften?

2. Har du hatt noen oppgaver/prosjekt/erfaring med multi-cloud og utvikling av ISP?

3. Har dere en egen gruppe som jobber med skytjenestene? (DevOps/CloudOps)

4. Hvor lenge har deres bedrift tatt i bruk skytjenester?

Del 2: Multi-cloud

1. Hva er dine tanker rundt multi-cloud (hybrid, cross), og hvordan det har påvirket deres bedrift?

   (a) Hva er det som gjør at flere og flere bedrifter går over til multi-cloud?
   (b) Er det noen spesifikke områder du ser som problematiske med tanke på sikkerhet?

2. Hva må bedrifter ta ekstra hensyn til med multi-cloud kontra single cloud?

3. Hvilke skylverandører tar dere i bruk? (Hva er de mest populære)

   (a) Er det noen spesifikke utfordringer med de ulike skymodellene/applikasjoner?

4. Kan du beskrive bedriftens multi-cloud sikkerhetsstrategi?

   (a) Utfører bedriften en risk assessment før implementering av skyleverandører, hvis ja, hvordan?
   (b) Er det noen form for mål av tiltakene for sikkerheten? (KPI)
   (c) Hvordan sørger bedriften for at alle standarder (NIST) og reguleringer (GDPR) blir fulgt?

5. Bruker bedriften noen form for (automasjon)verktøy/plattformer for effektivisering av multi-cloud?

6. Kan du drøfte over noe du har lært etter og ha implementert og jobbet med multi-cloud løsninger, som feks. best practices/fallgruver

Del 3: Utvikling av ISP (Policies)

1. Hva er din oppfatning av ISP? (Definisjon)

2. Hva mener du er viktig når man utvikler en ISP?

3. Bruker organisasjonen konsekvent en metode for utvikling av nye ISP?

   (a) Hvis nei - Hvorfor ikke (Outsourcing)?
   (b) Hvis ja - Dekker metodene det nødvendige, eller må man tilpasse de til organisasjonen?
   (c) Hvem blir involvert i denne prosessen?
   (d) Blir det basert på noe? (Internasjonale standarder eller strategi fra styret i bedriften, frameworks)

4. Er det nødvendig å innføre spesifikke ISP for multi-cloud i bedriften?
   (a) Hvis ja - Var det noe som skilte seg ut i utviklingsprosessen av ISP for multi-cloud i motsetning til single cloud/on-premise?
   (b) Hvordan sørger dere for at ISP er konsekvente gjennom alle leverandører?
5. Hvordan forsørger man at den tiltenkte målgruppen følger ISP?
6. Blir ISP revidert eller oppdatert i jevnlige intervaller?
   (a) Hvis ja - hva er det som utløser prosessen?
   (b) Hvis nei - hvorfor ikke?
7. Siste tanker?

Appendix C

Consent form

Informasjon om forskningsprosjektet

"Multi-Cloud security policy development framework"

I dette skrivet gir vi deg informasjon om målene for dette forskningsprosjektet og hva prosjektet innebærer for deg.

Formål

Dette er et masterprosjekt hvor formålet er å lage et rammeverk for å bedre sikkerheten til bedrifter som tar i bruk flere ulike skytjenester. For å klare å lage et slikt rammeverk trenger vi informasjon fra personer som jobber med dette, og kan gi oss deres erfaringer rundt dette temaet. Problemstillinger vi vil analysere er organisasjoners bruk av multi-cloud, ulike problemer dette kan/har ført til, samt generell forståelse rundt temaet. Opplysningene som blir samlet i dette prosjektet brukes kun til dette formålet.

Hvem er ansvarlig for forskningsprosjektet?

Thomas Øren og Sindre Pedersen Fosser er to studenter fra Universitet i Agder ved fakultet for samfunnsvitenskap og institutt for informasjonssystemer som er ansvarlig for prosjektet.

Hvorfor er du inkludert i studien?

Utvalget er i all hovedsak trukket ut ifra stilling og potensielle bedrifter som bruker flere skytjenester. Ettersom vår studieretning innebærer cybersikkerhet, vil det være relevant å intervjue kandidater som har en rolle innenfor dette feltet. Det er planlagt å sende ut så mange e-post invitasjoner som mulig i første omgang, for å se hvor mange som eventuelt kan stille på et slikt intervju. I utgangspunktet har vi tiltenkt å utføre omtrent 10-15 intervjuer.

Hva innebærer prosjektet for deg?

- Metoden vår for datainnsamling er kvalitative intervjuer, som vil bli gjennomført med digitalt opptak av lyd og bilde. Opplysningene som vi samler inn av intervjuobjektene er:
  - Navn
  - Stilling eller rolle i organisasjon
  - Informasjon rundt din stilling eller rolle i organisasjonen

- «Intervjuet vil vare i maks en (1) time hvor vi vil stille deg spørsmål som [Hva er din rolle i organisasjonen?] - [Hva slags fordeler/ulemper er medført med bruk av multi-cloud?] - [Har dere innført egne retningslinjer/policies knyttet til bruken av multi-cloud?]

Du kan protestere

Du kan når som helst protestere mot at du inkluderes i dette forskningsprosjektet, og du trenger ikke å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du velger å protestere.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Kun behandlingsansvarlige Thomas Øren og Sindre Pedersen Fosser vil ha tilgang til dine opplysninger.

- Kun behandlingsansvarlige Thomas Øren og Sindre Pedersen Fosser vil samle inn, bearbeide og lagre data.

- Tiltak for å sikre at ingen uvedkommende får tilgang til personopplysningene dine inkluderer;
  - Navn og kontaktopplysningene dine vil bli erstattet med en egendefinert kode som lagres på egen liste adskilt fra øvrig data. Et eksempel på dette vil være "*CloudEngineer*1" for en sky ingeniør i den første bedriften fremfor navnet på kandidaten.
  - Datamateriale vil bli lagret på en sikret OneDrive sky-konto under skolens [Universitet i Agder] domene med to faktor autentisering.
  - Personopplysninger vil bli lagret separat i en innelåst/kryptert mappe.

Deltakere vil ikke bli gjenkjent i publikasjon. Deltakere vil bli anonymisert og bli referert til som intervjuobjekt eller "*CloudEngineer*1". Organisasjonens navn vil også bli anonymisert. Av den grunn vil ikke noe informasjon kunne bli tilknyttet til deltakeren.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Etter endt prosjekt vil alt av oppbevarte data slettes, noe som etter planen er satt til 3.6.2023.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg fordi forskningsprosjektet er vurdert å være i allmennhetens interesse, men du har anledning til å protestere dersom du ikke ønsker å bli inkludert i prosjektet.
På oppdrag fra Thomas Øren og Sindre Pedersen Fosser har Sikt – Kunnskapssektorens tjenesteleverandørs personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

1. å protestere

2. innsyn i hvilke personopplysninger som er registrert om deg

3. å få rettet personopplysninger om deg,
4. å få slettet personopplysninger om deg, og
5. å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer eller å benytte deg av dine rettigheter, ta kontakt med:

- Institutt for informasjonssystemer ved Thomas Øren thomasor@uia.no og Sindre Pedersen Fosser sindrf16@uia.no og/eller førsteamanuensis Wael Soliman wael.soliman@uia.no ved Institutt for informasjonssystemer.
- Vårt personvernombud: Rådgiver/personvernombud ved IT-avdelingen: Trond Hauso trond.hauso@uia.no +47 936 01 625

Hvis du har spørsmål knyttet til vurderingen av prosjektet som er gjort av Sikts personverntjenester, kan du ta kontakt med:

- Personverntjenester på e-post (personverntjenester@sikt.no) eller på telefon: 73 98 40 40.

Med vennlig hilsen,

Sindre P. Fosser

Thomas Øren
Prosjektansvarlig

Sindre Pedersen Fosser
Prosjektansvarlig