UPPSALA
UNIVERSITET

UPTEC STS 23022
Examensarbete 30 hp
Juni 2023

Evaluating the Ownership of Personal Data in the Cloud by Optimizing the IT Architecture

Applying a reference architecture to make the ownership of personal data more clear within an organization

Sofie Hulteberg
Tilda Myrsell

Civilingenjörsprogrammet System i Teknik och Samhälle

UPPSALA
UNIVERSITET

Evaluating the Ownership of Personal Data in the Cloud by Optimizing the IT Architecture

Sofie Hulteberg
Tilda Myrsell

Abstract

Cloud computing is an area that many companies use in order to stay in line with technological development. To keep these systems productive and easily managed, a reference architecture can be used as a framework and also as a manual on how to structure an organization to suit its specific needs and goals. The reference architecture can make it easier to divide responsibility as well as working tasks within an organization. One company facing the challenges that comes with cloud based systems is Vattenfall, one of the biggest energy companies in Europe. An organization like Vattenfall handles a great load of customer data which is to be controlled and protected in every way. In order to keep on making sure that these systems are efficient and secure, a reference architecture could be a helpful tool.

With the purpose of investigating how a section within Vattenfall's IT department can use a reference architecture to determine the ownership of customers' personal data more easily, an interview study was conducted. The interviews focused on evaluation of how employees' reason when handling customers' personal data within cloud environments. The reference architecture found most suitable for handling personal data was the international standard ISO/IEC 17789. It describes multiple work roles within cloud computing which can make the process of handling sensitive information clearer and easier. The data collected from the interviews was later applied to this reference architecture in order to see how it can be used in order to more easily divide responsibility. The study could in the end present several recommendations as to how the department should divide responsibilities and raise awareness regarding the topic amongst employees in order to increase data security.

Finally, the expected value created from implementing these recommendations and applying the reference architecture to the organization is expected to be high. The thesis concluded that the chosen reference architecture can be applied to the Vattenfall organization. With a few organizational changes, the responsibility regarding customers' personal data can be divided more easily amongst the employees and the security can be improved. The recommendations presented could benefit the organization and raise awareness of the topic amongst employees.

Teknisk-naturvetenskapliga fakulteten

Uppsala universitet, Utgivningsort Uppsala/Visby

Handledare: Yasith Wickramasinghe Ämnesgranskare: Davide Vega D'Aurelio

Examinator: Elísabet Andrésdottir

Acknowledgement

We would like to take this opportunity to thank everyone who played a significant role in our Master Thesis project. This study was done in collaboration with Vattenfall as a part of the Sociotechnical Systems Engineering program (STS) at Uppsala University.

Firstly, we want thank our supervisor at Vattenfall, *Yasith Wickramasinghe*, without you this study would never have been possible. Thank you for your guidance, support and the happy memories from the whole process. We also want to thank our subject reviewer *Davide Vega D'Aurelio* for his valuable advice and inspiring words which has been much appreciated.

Lastly, we want to thank all the employees at Vattenfall who participated in the interview study and their commitment to the topic. We are grateful for your thoughts and interest in our master thesis project.

Sofie Hulteberg & Tilda Myrsell
May, 2023

Populärvetenskaplig sammanfattning

Många företag använder sig av molntjänster för att kunna hålla sig i linje med den tekniska utvecklingen i samhället. För att upprätthålla produktiviteten och ha lätthanterliga system så kan en referensarkitektur användas som ramverk. En referensarkitektur kan användas som en manual för att strukturera en organisation så dess uppbyggnad passar specifika behov och mål. Med hjälp av en referensarkitektur kan det också bli enklare att fördela ansvarsområden samt arbetsuppgifter inom en organisation. Ett företag som står inför utmaningar som kommer med molnbaserade system är Vattenfall, ett av de största företagen inom energibranschen i Europa. En organisation likt Vattenfall hanterar stora mängder kunddata som måste kontrolleras och skyddas på alla sätt. För att säkerställa att de system som hanterar dessa typer av data fortsätter vara effektiva och säkra kan en *referensarkitektur* vara hjälpsam.

Studiens syfte är att undersöka hur en del av Vattenfalls IT avdelning kan använda en referensarkitektur för att enklare fastställa ägandeskap av kunders personliga data. För att kunna svara på detta, genomfördes en intervjustudie. Intervjuerna fokuserade på evaluering gällande hur anställda hanterar kunders personliga data inom molnbaserade system. Parallellt med intervjustudien så studerades referensarkitekturer för att hitta en struktur som passade för det specifika fallet. I slutändan konstaterades det att den referensarkitektur som ansågs vara mest passande för hantering av personlig data var den internationella standarden *ISO/IEC 17789*. Denna referensarkitektur beskriver flertalet arbetsroller inom molntjänster vilket kan göra hanteringen av känslig information tydligare och enklare. Senare applicerades den valda referensarkitekturen på datan insamlat från intervjuerna. På detta vis kunde potentiella luckor identifieras samt en bild skapas av hur man enklare kan dela upp ansvaret. Om anställda har tydligt beskrivna ansvarsområden så kan ägandeskapet beskrivas tydligare och dataflödena kan bli enklare att uppfatta. Studien kunde i slutändan presentera ett antal rekommendationer gällande hur avdelningen bör dela upp ansvaret och öka medvetenheten av ämnet bland anställda, vilket även är ett sätt att öka datasäkerheten på.

Slutligen, genom att applicera referensarkitekturen på Vattenfalls IT avdelningen och implementera det föreslagna rekommendationerna förväntas det genererade värdet för Vattenfall bli högt. Studien konstaterar att den valda referensarkitekturen kan appliceras på den relevanta avdelningen inom Vattenfall IT. Genom några få organisatoriska förändringar så kan ägandeskapet gällande kunders personliga data fördelas enklare mellan de anställda och säkerheten kan öka. De presenterade rekommendationerna kan gynna organisationen och öka medvetenheten om ämnet bland de anställda.

Abbreviations

CCRA – Cloud Computing Reference Architecture

CSC – Cloud Service Customer

CSC: administrator – CSC: Cloud service administrator

CSC: business manager – CSC: Cloud service business manager

CSC: integrator – CSC: Cloud service integrator

CSC: user – CSC: Cloud service user

CSN – Cloud Service Partner

CSN: auditor – Cloud service auditor

CSN: broker – Cloud service broker

CSN: developer – Cloud service developer

CSP – Cloud Service Provider

CSP: business manager – Cloud service business manager

CSP: customer support and care representative – Cloud customer support and care representative

CSP: deployment manager – Cloud service deployment manager

CSP: inter-cloud provider – Cloud inter-cloud provider

CSP: manager – Cloud service manager

CSP: network provider – Cloud network provider

CSP: operations manager – Cloud service operations manager

CSP: peer provider – Peer cloud service provider

CSP: security and risk manager – Cloud service security and risk manager

GDPR – The General Data Protection Regulation

ISO/IEC – ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission)

NSI – National Security Information

PII – Personally identifiable information

RA – Reference architecture

SLA – Service Level Agreement

VIT – Vattenfall IT

YIA – Vattenfall Customer IT

YIAS – Vattenfall Customer IT Sweden, a sub-department to YIA who handled the Swedish part of the business.

Table of Contents

1. Introduction

This project consists of an analysis of Vattenfall's cloud enterprise architecture. A cloud environment constructed by the department *Vattenfall Customer IT (YIA)*[1] Sweden will be examined and evaluated. The main focus of the work is the ownership and security of personal data since there is a need within the department for such an investigation.

Vattenfall is a Swedish energy company with approximately 19 000 employees and more than 100 years of experience supplying customers with electricity and heat (Vattenfall, n.d.). Vattenfall is determined to achieve the goal: "enable fossil-free living in one generation" and in order for this to succeed, Vattenfall is currently working on new and sustainable solutions to electrify society (Vattenfall IT, 2020). In 2022, the issues of prices within the electricity market and access to energy were main topics and Europe was presented to an unknown situation. According to the Vattenfall Press Office, it has now become clear that Vattenfall plays a key role in society (Vattenfall Press Office, 2022). Therefore the organization requires reliable and trustworthy IT solutions. According to *Vattenfall IT (VIT)*[2], cloud computing plays a big role since it is at the forefront of technology today and therefore is needed within a modern company. Implementing cloud solutions is one of the main tasks of the IT department within Vattenfall as they can be used to optimize operations and drive new business areas (Vattenfall IT, 2020).

Cloud services have been used at Vattenfall for several years. The importance of new solutions has resulted in an accelerated development of cloud technology within the company. It has led to an increase in value for multiple different business areas, such as customer online services and more predictive maintenance of the company's assets. The use of cloud technology is not a strategy in itself, but exploiting the value and possibilities of cloud technology which according to Vattenfall gives the company a competitive advantage in the market (Zimmermann, et al., 2018). Vattenfall has, for several years, embarked on a cloud transformation journey and is now prominent within the energy industry when it comes to IT solutions. Vattenfall also has a "cloud first" strategy which is to be considered in all business related decisions. When implementing new or when changing already existing IT solutions the use of cloud technologies should always be taken into consideration (Krüger, n. d.). Cloud services are therefore a fundamental technology for one of the biggest energy companies in Europe (Vattenfall, n.d.).

Vattenfall describes IT as the backbone of the business and an area which has a significant part in achieving the company's goals. In order to optimize the operations within the department, a stable IT infrastructure is required. Information security is of most importance and VIT needs to make sure that the data is stored securely and can be

[1] YIA is Vattenfall's internal name for the department Vattenfall Customer IT (Vattenfall Customer IT, 2023).
[2] VIT is an abbreviation of Vattenfall IT (Zimmermann, et al., 2018).

accessed quickly when needed. Combining this business goal with the development of stable cloud services provides the company with a powerful combination which can be used to drive technological development even further. The around 900 000 customers that Vattenfall are supplying with electricity each day are relying on the company to keep their personal data safe and prioritized (Eldistribution, n. d.). In order to maintain this, the cloud architecture has to be well-developed and updated to satisfy the end users' needs (Vattenfall IT, 2020).

Interestingly, an example to how system security can be affected actually took place whilst this project was being conducted. In February of 2023, Vattenfall and a number of other organizations were exposed to cyber-attacks which were directed towards Swedish infrastructure. The attacks were so called overload attacks and affected the official website Vattenfall.se and made it unavailable for users during a limited amount of time (Dagens Industri, 2023). This proves the importance of safe and secure systems that are up to date with technological development. Since Vattenfall handles big amounts of personal data that have to be protected at all times. The company handles personal data to develop useful products for their customers but also to the business itself. *The General Data Protection Regulation (GDPR)*[3] requires companies to protect personal data and be transparent on how they process it. This is also a fundamental right to all European citizens. Therefore the protection of customers personal data is a daily challenge for a company like Vattenfall and staying in line with implemented laws is now a fundamental part of the organization's daily work (Noushandeh, 2017). In order to maintain the security of the digital systems, VIT is in need of an evaluation of its enterprise architecture.

Hence a *reference architecture (RA)*[4] can be used to help the organization realize what improvements are possible. By performing an interview study with relevant employees regarding how staff reason when handling these types of data, a dataset will be collected. The cloud environment has also been studied in order to get an idea of how it is structured today. By performing a discourse analysis, the answers from the interviews will be analyzed and later applied to the set RA. By doing so, the lack of specific responsibilities can be identified and it will also make sure that the personal data is kept safe and the ownership of it is clearly stated. This method will provide recommendations as to how the RA at YIAS can be structured in order to determine the ownership easier as well as protect the sensitive types of data.

[3] GDPR is an abbreviation of The General Data Protection Regulation which is the EU's general Data Protection Rules (Noushandeh, 2017).
[4] RA is an abbreviation of reference architecture which is a template for designing digital systems (Wipf, 2023).

1.1 Purpose and Research Questions

The purpose of this master thesis is to investigate the Swedish part of the cloud environment at *Vattenfall Customer IT Sweden (YIAS)*[5] focusing on determining the ownership of personal data. By the usage of the international standard for cloud architecture – the RA named *ISO/IEC 17789*[6], gaps between the already existing cloud architecture and the recommended one can be identified. Since this framework for cloud architecture focuses on the security of personal data it can be used for determining the ownership. By creating a recommendation for how the cloud architecture should be built to keep the ownership of the personal data clear, YIAS can improve its cloud solutions and business goals. It will also help the department to more easily achieve its own purpose.

Therefore, the following research questions will be investigated:

- *How can a cloud environment architecture be organized in order to handle personal data?*
- *What actions can increase the security of personal data in the cloud environment within YIAS?*

As discussed previously, this thesis will explain how customers' personal data is stored and processed in the YIAS department. We will examine the research questions stated above by performing a literature study as well as internal interviews with employees. In this way, we can provide YIAS with a recommendation and improvements of how the organization can handle customers' personal data and the security aspects of it. We will also include a proposition of how the organization could be structured in order to achieve this easier.

1.2 Limitations

Since this master thesis was set during a time period of 20 weeks, it was performed with limitations. Vattenfall is an international company but this project has only focused on the Swedish market which means only Swedish systems will be evaluated. Analyzing the cloud environment of the whole company Vattenfall as well as other YIA sub-departments was considered too big of a workload for the limited time period. Further, the project has exclusively analysed the current state of the cloud environment as of January to June 2023. Past and future versions of the platform was therefore not evaluated in this study.

[5] YIAS is an internal abbreviation of YIA Sweden (Vattenfall Customer IT, 2023).
[6] ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. Nations that are members of ISO or IEC participate in the development of International Standards through technical committees to address specific areas of technical activity (International Organization for Standardization, 2014).

The RA being used in this project is the ISO/IEC 17789 which includes a number of responsibility roles within an organization. In order to follow this RA, these roles should exist in the organization where the framework is being applied (International Organization for Standardization, 2014). In order to keep the scope of the project to personal data security and ownership, some roles have then been eliminated in the framework, since they were considered not relevant for the scope of the project.

Only cloud solutions within Microsoft Azure were analyzed since they are Vattenfall's preferred cloud service provider based on an enterprise agreement. This strategic decision regarding technology provides the opportunity to leverage synergies in partnership with Microsoft, while limiting the effort associated with activating and managing multiple external cloud service providers (Zimmermann, et al., 2018).

2. Background

In the following section, the structure of the department YIA will be described as well as its sub-department YIAS. Aspects such as the departments' purposes, organizational structures and way of working will be explained. The following paragraphs will also explain the concept of RA and how it can be a beneficial tool for organizations. How Vattenfall as an organization works with and handles data security will also be reviewed.

2.1 Introducing Vattenfall Customer IT and Vattenfall Customer IT Sweden

The main purpose of the YIA department is to: "drive the technology behind one customer experience across Vattenfall". The department is successful in building and running Vattenfall's end-user software through close cooperation with business departments, developing secure IT solutions. All these aspects are important in order to keep the cloud solutions up to date and secure to make customers' personal data safe. In order to achieve this, a suitable RA for cloud services is essential. To understand the structure of the organization, the following section will focus on YIA, see Figure 1 (Vattenfall Customer IT, 2023). In Figure 1 the whole department of YIA can be viewed. It covers all sub-departments and the main roles belonging to the division. Here, YIAS is also marked in a lighter blue colour to emphasize the importance of the structure for this specific project.

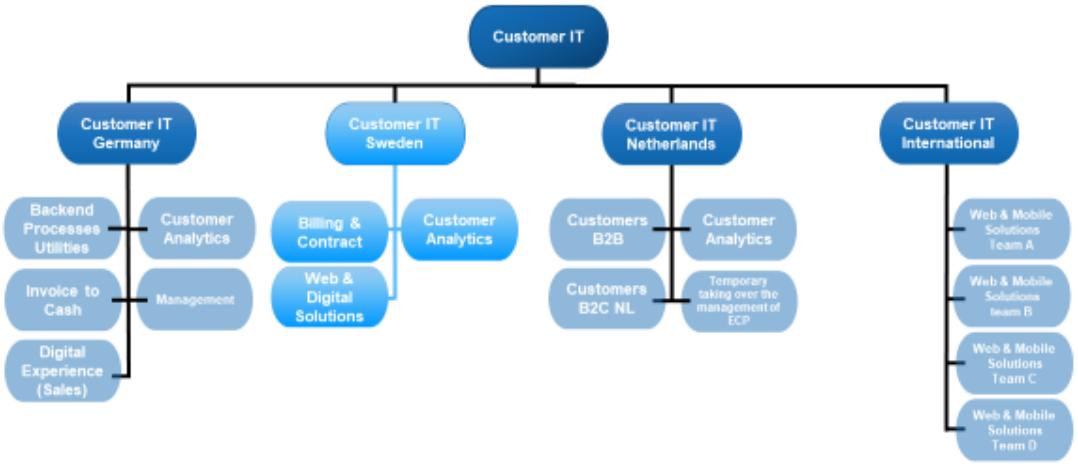

Figure 1. The YIA department and associated sub-departments (Vattenfall Customer IT, 2023).

YIA is responsible for building and running Vattenfall's end customer software. This involves programs such as the Vattenfall intranet and the main website Vattenfall.se. The department is also responsible for solutions such as customer relationship management and a selling and information system specific for companies within the energy industry and customer data analytics. The main purpose of the department is to run and build

software for all business areas. Top priorities are close cooperation with its business colleagues to deliver customer value and improve customers' digital experiences (Noushandeh, 2017).

The department itself is divided into four different sub-departments where each group is responsible for different areas which are supervised by a manager. The geographical areas of activity are: Germany, Netherlands, International and Sweden. The sub-department YIAS is focusing on the Swedish market and this manager is in turn responsible for three smaller teams where each has an accountable person as well. The business areas covered are: Billing and Contract solutions, Customer Analytics along with Web and Digital Solution. These teams have different responsibilities but work together across the department. The YIAS department plays a big role in developing Vattenfall.se since it manages both parts of the website but also the MyPages functionality. This is where customers log into their accounts in order to see invoices and contracts. This means that the department handles big amounts of customers' personal data and have fundamental assignments (Vattenfall Customer IT, 2023).

2.1.1 User Case

In order to understand the complexity and importance of this topic, a user case will be used throughout the thesis. This will provide the discussion with a context and also help us explain certain concepts and challenges that can surface when working with this subject. This user case has also been mentioned by multiple employees who participated in the interview study. In Appendix A, all participants of the interview study are compiled into Table 3. Some interviewees explain that YIAS is responsible for keeping personal data safe and secure. This can be confusing at times since the ownership in accordance to customers' personal data is not always stated or clear. When working with customer integrated systems, this can sometimes cause complications in the processes. E.g., imagine that a previous customer makes a call to Vattenfall and asks the company to delete all the customers' personal data which has been stored digitally in the organization's systems. This could be customers' personal accounts and according to legislations, a customer has the right to have this removed if requested. The problem here is that in many cases, it is not clear who owns the personal data and therefore can perform the task. In addition, if an employee was to delete all the data and the ownership was not clear it might be deleted from one system but the operation might not be carried out further down the line in connected structures. The main problem with this procedure is that traceability of changes is hard to document. Since this means that it is hard to know if the wish of the customer has been carried out correctly or not. According to GDPR, there are rules regarding how often customers' personal data should be updated in different systems as well as when it should be deleted if not used for a specific amount of time. It is also stated that if a customer wants to have all their personal data removed from a company that stores it, they have a legal right to have this performed by the company (Svensson, 2023a). This could mean that a company is not acting in accordance to GDPR if they

cannot honestly state that the customers' data has been removed from all places where it was being stored, if this is the request of the customer. Making sure that the ownership of customers' personal data in digital systems is stated clearly and the responsibilities are divided between employees accordingly, this situation can be avoided. Therefore clear ownership of customers' personal data within a company cannot be emphasised enough.

2.2 Reference Architecture as a Tool for Organizations

In order to design reliable software architectures, an RA can be a helpful tool for a company. According to multiple studies it is well known that when developing digital systems it can over time be difficult abiding by one type of framework. If a digital system is developed over many years complications can occur as employees come and go at the company. If each of these employees were to handle the system in their own way without guidelines the system can over time become difficult and unorganized to handle. An RA provides the design pattern which could help a company avoid such a situation. IT and cloud architects use the RA as a starting point when developing systems and a blueprint which they always can come back to (Galster & Angelov, 2015). It also provides the architects with knowledge regarding design of a software system as well as specific tactics and patterns that should be used (Abbas & Andersson, 2015). It is also helpful for corresponding the intended design of the system to future employees who will be working on it. Architectural decay can be costly for a company as it affects the system's reliability and dependability since processes might turn ineffective compared to earlier in the systems lifetime. In conclusion, working on a technical system without an architectural framework may turn into a time-consuming, costly and difficult process (Medvidovic, 2015).

RA as a tool can be specifically beneficial for a company who has implemented an agile way of working. For many years there was an ongoing debate whether agility and RA could coexist as working methods. Nowadays, most experts are convinced that it is possible and that RA can be suitable for an agile organization. Since Vattenfall uses an agile way of working, this reasoning can be applied to the company. It is recommended that architectural decisions are made early on in a project since it makes it easier to continuously follow the decided RA. Since many other decisions along the line of a project depend on the architectural design of the relevant software. If an organization e.g. was going to perform updates or developments on an already established digital systems it can be helpful to have a blueprint as to how it was designed. This blueprint may also include the original developers' future plans for the system (Abrahamsson, et al., 2010).

The focus on quality attributes within software architectures can lead to improvements of projects executed with agile methods (Nord & Tomayko, 2006). An RA is also especially helpful in large-scale agile projects since it facilitates communication, documentation and validation (Lindvall, et al., 2002); (Cantone & Alessandro, 2010). Another reason RA can be a helpful tool in agile projects is because it speeds up the design work and ensures

reusability of designs. This way cost can be reduced since it saves both resources and employee related costs. The main downside of this combination of working methods is that if the organization is heavily agile oriented it can affect the maintenance of already existing RA. Since there may not be enough resources in an agile working method to maintain already existing solutions and designs. Agile methods are mostly focused on creating customer value and RA maintenance do not offer a direct connection to this. It is usually used to create a bigger value for the software developing company than the actual end-customer (Galster & Angelov, 2015).

2.3 Personal Data Protection

Personal data is data that can be traced directly or indirectly to an individual person, such as name, address and place. A personal data breach is a breach of the safekeeping of personal data such as its loss, theft or unlawful processing (Noushandeh, 2017). GDPR makes it possible for the customer to control their own personal data. The user case mentioned in section 2.1.1 regarding the customer asking to have their personal data deleted becomes relevant here. This is one of the fundamental rights of a customer stated in the GDPR legislation (Svensson, 2023a). In order for Vattenfall to easily follow GDPR, the company follows a privacy vision and mission. The customers, employees and business partners must be able to rely on Vattenfall handling and controlling their personal data correctly. The principles connected to this require Vattenfall to be able to show transparency on how the personal data is handled and what processes they are a part of (Svensson, 2022).

The data has to be classified according to Vattenfall's information asset classification. The asset evaluates the data in accordance to how much it would affect the company if the data was not secure or handled in a correct way. VIT has a number of legislations that have to be followed in order to process data in the cloud. Since Vattenfall is an international company, different requirements apply in different countries. The *National Security Information (NSI)*[7] includes requirements that are specific for moving information outside of the country's borders. The laws controlling this can be very different but the main aspect they have in common is that they are so highly critical that the security requirements cannot be matched with a cloud solution (Zimmermann, et al., 2018).

It is also mentioned that according to the Vattenfall legal department a Controller has to be named for all pieces of personal data. This employee has the ultimate responsibility for the personal data and all external companies that might have to process it do so on behalf of the controller. Relevant laws such as GDPR depend on the role of controllers and would not be applicable if these were not appointed (Zimmermann, et al., 2018). In

[7] NSI is an abbreviation of National Security Information (National Institute of Standards and Technology (NIST), u.d.).

addition to GDPR, Vattenfall also follows the *SCHREMS II*[8] legislation. As a consequence of this, Vattenfall is only allowed to make data transfers to or accessible from a third part outside of the European Union if the security can be ensured. Vattenfall as a company has to be able to make sure that the personal data is protected and prevented from large scale data processing foreign organizations. This means that Vattenfall is utterly responsible for the personal data during the whole process. The legal department at Vattenfall has started a project which is called SCHREMS II, in order to make the coordination of this framework easier for the organization. The project involves aspects such as how to handle personal data processing outside of the European Union that is in production already (Svensson, 2023b).

2.3.1 Personal Data Protection in a Vattenfall Context

As mentioned earlier, VIT handles a large quantity of personal data. In order to keep this information sorted and easily accessed by the employees it has to be classified when entered into the relevant systems. When entering the data into the cloud service a specific legal constraints are taken into consideration. The higher the security requirement, the higher the security. Therefore a private cloud is to be preferred since this makes it possible to reduce the security risks (Zimmermann, et al., 2018). The data protection work at Vattenfall is organized according to a three lines model, used for management and control of risk in general. The model secures the responsibility of handling personal data through different roles: 1. Risk ownership, 2. Independent monitoring as well as 3. Assurance. The lines themselves have the following structure.

1) The first line consists of *Data Protection Coordinators (DPC)*[9]. These employees are responsible for the implementation of policies and instructions on data protection. They are responsible for making sure that the requirements are being followed within the organization.
2) The second line is made up of *Data Protection Officers (DPO)*[10] and *Group Data Protection Lead*. The data protection officers main task is to assist the management at Vattenfall with legal advice, risk evaluation and standards. The group data protection lead has the responsibility to document the data protection work and make sure that it is accessible through the organization.
3) The third and last line of defence is the *Internal Audit*. The main task for this line is to provide Vattenfall with services designed to improve the all over operation (Svensson, 2022).

There are high risks when dealing with personal data. The consequences of a failure can affect the whole company and lead to economic loss. It could also harm the trust of the customers and stakeholders which could have great effect on the organization.

[8] SCHREMS II is an extension of the GDPR legislation (Svensson, 2023b).
[9] DPC is an abbreviation of Data Protection Coordinator (Svensson, 2022).
[10] DPO is an abbreviation of Data Protection Officer (Svensson, 2022).

Vattenfall's approach to data protection is in accordance with the guidelines provided by the current data protection legislations. In practice this means that Vattenfall's strategy for data protection is so called "risk based". This means that the controller should prioritize reducing the higher risk and make sure that the relevant actions required are being done. If the controller decides to use the personal data in a process or service the ownership might be passed on to a processor. If this is the case, the processor needs a written contract, a Data Processing Agreement. This contract is important to make sure that both parts understand the responsibilities involved in handling personal data within an organization (Svensson, 2022).

3. Theoretical Framework

In this section, a review performed on the topic of RA is presented. In connection to RA, this part of the thesis also covers the international standard ISO/IEC 17789 and why it is considered a suitable framework for this specific case.

3.1 Reference Architecture

There has been a great amount of research being done on the area of using an RA within organizations and what benefits and disadvantages exist with the method. Many studies have also taken the aspects of personal data into consideration. Weyns, Mirandola and Crnkovic (2015) collected the results of the 9th European Conference on Software Architecture into a systematic review on RA within software and cloud development. Here many studies have been gathered which serves a valuable ground for future research within the subject (Weyns, et al., 2015).

Galster and Angelov (2015) describes the usage of RA within a company and its benefits. Their project was conducted as a case study with two investigated cases. Here the authors investigated how well the usage of RA is suited for larger companies developing software systems. The data consists of interviews in combination with organizational understanding and system analysis of the ongoing projects. The authors came to the conclusions that RA can help with effectivization of processes when developing digital systems. The use of RA can benefit to organizations working with software development since it makes it easier for projects to abide to the original plan. It also contributed to the companies employees having a more general picture of the different groups ongoing work and though processes. Therefore the study can conclude that using RA is beneficial for an organization and can help with avoiding certain complications in development (Galster & Angelov, 2015).

As a complement to this, another study written by Angelov et al (2008) can be helpful. In this study, Angelov et al describes the process of modifying an already existing RA to suit a case better. This is mainly done through removing, replacing or altering responsibility roles described in the relevant RA. The authors describe how an RA can be evaluated and therefore designed into matching a specific case. The principle of mapping a current architecture to the RA still applies but irrelevant working roles are removed to get a clearer picture of the discussion. It also makes it easier to determine what responsibility roles are more important and relevant to the specific case. All RAs are not applicable on all systems and organizations so an evaluation has to be made before starting a study. The more relevant aspects of an organization have to be identified in order to modify the RA you are comparing to (Angelov, et al., 2008).

3.2 The International Standard ISO/IEC 17789

The international standard ISO/IEC 17789 from now on called the *standard* specifies the *Cloud Computing Reference Architecture (CCRA)*[11], which includes cloud service roles, cloud service activities and cloud service functional components and their relationships. The CCRA focuses on the requirements around "what" cloud services are providing and not on "how" to design cloud-based solutions. CCRA is a general architecture for systems and not for a particular cloud service system although it may constrain a specific system. CCRA can be applied to different products, services or reference implementations and the architecture does not define solutions that lead to inhibiting innovation (International Organization for Standardization, 2014, p. 3)

This International standard describes CCRA from four different viewpoints:

1) The *User view* includes the system context, parties, roles, sub-roles, and the cloud computing activities.
2) The *Functional view* shows the necessary functions for the support of cloud computing activities.
3) The *Implementation view* describes the functions that are necessary for the implementation of a cloud service within service parts and/or infrastructure parts.
4) Lastly, the *Deployment view* shows how the functions of a cloud service are technically implemented within an already existing infrastructure or within new elements to be introduced in this infrastructure (International Organization for Standardization, 2014, p. 4).

Not all layers or functional components are necessarily instantiated in a specific cloud computing system (Cyber risk countermeasures education, 2021). Those functions that span across multiple layers are called *multi-layered functions*. The multi-layer functions comprise a set of functional components that interact with functional components in the other four layers above to provide support functions, including, but not limited to, Integration, Security systems, Operational support systems, Business support systems and Development function (International Organization for Standardization, 2014, p. 8).

Whitin CCRA we have four different roles:

1) The first role is *Cloud Service Customer (CSC)*[12] which is a part that has a business relationship to users of cloud services.

[11] CCRA is an abbreviation of Cloud Computing Reference Architecture (International Organization for Standardization, 2014).
[12] CSC is an abbreviation of Cloud Service Customer (International Organization for Standardization, 2014).

2) The second role is *Cloud Service Provider (CSP)*[13] which makes cloud services available.
3) The third role is *Cloud Service Partner (CSN)*[14] which supports and assists the activities conducted by the CSP and the CSC.
4) Finally the fourth role *Peer Cloud Service Provider* is a cloud service provider who provides one or more cloud services for use by one or more other cloud service providers as part of their cloud services. Within these four roles, there are sub-roles that divide the activities (International Organization for Standardization, 2014, p. 6).

3.2.1 Responsibility Roles of the Reference Architecture

Within the RA there are a number of different responsibility roles that correlates to employees within an organization. As can be seen in Figure 2, the different roles are divided into sections covering different areas within cloud computing.

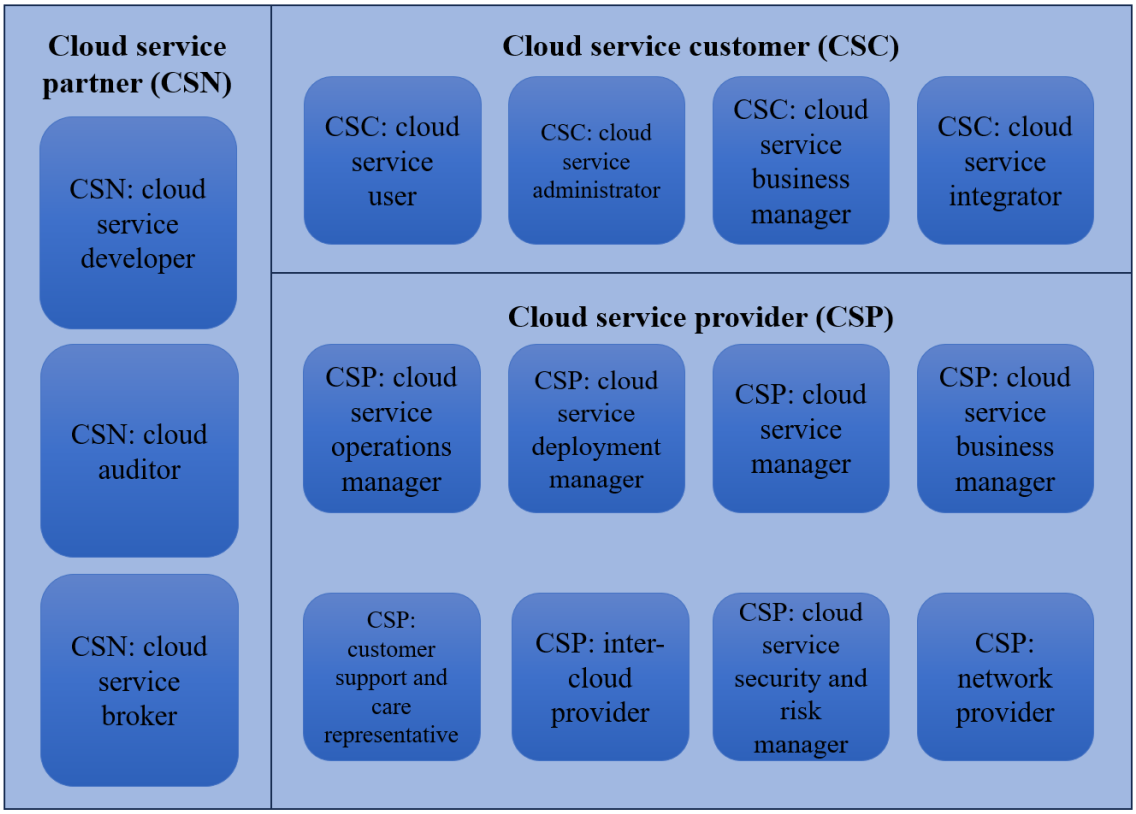

Figure 2. The different responsibility roles within the RA ISO/IEC 17789 (International Organization for Standardization, 2014, p. 10).

[13] CSP is an abbreviation of Cloud Service Provider (International Organization for Standardization, 2014).
[14] CSN is an abbreviation of Cloud Service Partner (International Organization for Standardization, 2014).

Within the section ***Cloud Service Customer CSC*** there are four different responsibility roles:

- A *CSC: user* corresponds to a natural person or an entity that is associated with a cloud service customer that uses cloud services.
- A *CSC: administrator*'s main goal is to ensure the smooth operation of the customers' use of cloud services and that those cloud services are running well with the customers' existing *information and communication technology (ICT)*[15] systems and applications. The operational processes are monitored by the administrator and this person also acts as the point of contact for the technical communication between the cloud service customer and the cloud service provider.
- A *CSC: business manager* role aims to meet the business objectives of the cloud service customer by adapting and using cloud services in a cost-efficient way. The main responsibilities of this role concern financial and legal aspects of the cloud services which includes ownership and accountability.
- A *CSC: integrator* is responsible for the integration of cloud services and works with customers' existing ICT systems in the cloud service (International Organization for Standardization, 2014, pp. 10-11).

Under ***Cloud Service Provider CSP*** there are eight different sub-roles described below:

- A *CSP: operations manager* main task includes making sure all operational processes and procedures of the CSP are performed.
- A *CSP: deployment manager* plans the deployment of a service that is going into production. The responsibility includes defining the operational environment of the service, the initial steps and dependencies for deployment and activation of operations processes used.
- A *CSP: manager* is responsible for ensuring that the CSP's services are available for use by cloud service customers. To ensure that the functions work correctly and meet the objectives set out in the SLA. The manager is also responsible for ensuring that the CSP's business support systems and operational support systems are running smoothly.
- A C*SP: business manager* has overall responsibility for the business aspects of offering cloud services to cloud service customers. This role defines the strategy and business plan and manages the business relationship with cloud service customers.
- A *CSP: customer support and care representative* is responsible for ensuring customer satisfaction with the cloud service provider and handling customer issues in a timely and cost-effective manner.

[15] ICT is an abbreviation of information and communication technology (International Organization for Standardization, 2014).

- A *CSP: inter-cloud provider* works with intermediation, aggregation, arbitrage, peering or federation of peer providers' cloud services and their business and administration capabilities from the cloud service customer viewpoint.
- A *CSP: security and risk manager* main responsibilities include ensuring that the cloud service provider adequately manages the risks associated with the development, delivery, use and support of cloud services. Includes ensuring that the information security policy of the cloud service customer and the cloud service provider is appropriate and meets the security requirements set out in the SLA.
- A *CSP: network provider* ensures that network connectivity and network services are provided for the cloud service customer, partner and provider (International Organization for Standardization, 2014, pp. 14-15).

The CSP: service manager sometimes provides its service in collaboration with another CSP: service manager. In this case, the cloud service invokes the other service provider. This is described as a provider to ***Peer Cloud Service Provider CSP*** relationship, or alternatively as an "inter-cloud" relationship. Hence the provider making use of the services is therefore called a primary cloud service provider while a provider whose services are being used is termed a secondary cloud service provider. The role of the *CSP: service manager* is in this case to manage peer cloud services to establish contracts and SLA's for the use of the peer cloud service (International Organization for Standardization, 2014, p. 21).

Within ***Cloud Service Partner CSN*** there are three different sub-roles which are:

- A *CSN: developer's* main responsibilities include designing, developing, testing and maintaining the implementations of a cloud service.
- A *CSN: auditor* is responsible of conducting an audit of the provision and use of cloud services. An audit of cloud services typically covers operations, performance and security and examines whether a certain set of audit criteria are met.
- A *CSN: broker* negotiates relationships between cloud service customers and providers. The main tasks are acquiring and assessing customers, accessing the marketplace and drawing up legal agreements such as GDPR legislation, but the role is not involved when the service is in use (International Organization for Standardization, 2014, p. 21).

3.2.2 Common Roles, Activities and Functional Components

In Figure 3, the CSP has a sub-role. This means that the CSP's service manager performs the provision of service activity. This then provides the service which the CSC's user of the cloud service customer can use. Although, before this service can be used, the cloud service needs to be developed and deployed in order to be operational. In this case, two sub-roles of cloud service partners are involved – the developer and auditor. The developer develops the implementations of the cloud services by using the development

tools functional component and also tests the service using the test management functional component (International Organization for Standardization, 2014, p. 40).

After the CSP's service manager performs the deploy and provision services activity, the provide services activity uses the service provision functional component. This is the implementation of the service, which in turn uses the resource layer functional components for the compute, storage and network resources required to run the service. The integration of the service capabilities functional component with the functional security component also makes the service provision activity. This is done by using the security systems functional component and protection functions for personally identifiable information capabilities, such as data encryption. In operational support systems, the functional component supports the management, monitoring, automation and configuration of services and resources. It is also the CSP's service manager that manages the service level of the platform. To ensure that the objectives defined in the *Service Level Agreement (SLA)*[16] applicable to the cloud service are met, the Service Level Management activity manages the availability and performance of the cloud Service. Therefore, the Service Level Management, Monitoring and Reporting, and Incident and Problem Management functional components are used to achieve this – the objectives defined in the SLA which applies to the cloud service which is high security for personal data (International Organization for Standardization, 2014, p. 41).

When a cloud service is available for use, there are two sub-roles for service customers that perform different activities. It is then the CSC: administrator that performs the lease administration activity using the administrator function component. This is done to configure the lease relationship to grant access rights to the CSC: users. When this is done, CSC: users perform the activity using the cloud service and the user function component to be able to interact with the cloud service. At the same time, CSC's administrator monitors the service to ensure that it is working properly and meets the terms of the SLA. Again, this is done using the administrator function component (International Organization for Standardization, 2014, p. 41).

3.2.3 Protection and Ownership of Personally Identifiable Information

The CSP is a section within the standard that includes multiple responsibility roles. This section should be the one to protect the assured, proper and consistent collection, processing, communication, use and disposition of *personally identifiable information (PII)*[17] when using cloud services. According to the framework, one of an organization's key business imperatives is to ensure the protection of PII. This can be done through cloud computation which provides an adaptable solution for shared resources, software and

[16] SLA is an abbreviation of Service Level Agreement (International Organization for Standardization, 2014).
[17] PII is an abbreviation of Personally Identifiable Information (International Organization for Standardization, 2014).

information. Cloud computing presents additional confidentiality challenges to CSC that uses cloud services but also to cloud service providers. Since there are strict jurisdictions and requirements that apply to the handling of PII it presents itself with many challenges. This since any use of cloud services to store and process PII often has to follow these regulations (International Organization for Standardization, 2014, p. 26).

In general, the responsibility role considered to have legal ownership or control over the PII is considered to be the owner of it. In the case of the RA, this responsibility is described to lay with the CSC. Since part of the managing as well as some legal aspects can be found in this part of the RA the ownership of PII within a cloud system could be suitable to place here. The CSC is responsible for ensuring that any pieces of data that contain personal information is stored correctly. The standard emphasizes the importance of being compliant with relevant laws and jurisdictions. Since the CSC is usually responsible for ensuring this compliance it further strengthens the perception if the CSC being the owner of customers' PII in the cloud. So, from a legal standpoint, they can be considered as the data owner. However, according to the standard, the CSP also plays a key role in the ownership of PII. Although this role is usually not considered responsible for the content of data. The role is instead described as being in charge of providing the necessary infrastructure and controls to protect the data from unauthorized access. This suggests that the CSC may have greater ownership or control over the relevant data. Ownership of PII in the cloud is complex and specific responsibilities of the CSC as well as the CSP are dependent on the circumstances and structure of the organization where it is being applied. According to the standard the most important task is to establish clear responsibilities between working roles no matter who is considered as the owner of personal data. Within information security, there are several different standards that can be used for auditing system security. The jurisdiction for handling PII usually differs from country to country. One of the issues which can occur, connected to the cloud service is that the CSC can be in a different jurisdiction to that which applies to the CS. The situation can become increasingly more complex if the CSP operates multiple data centres in different jurisdictions and moves data between these data centres. ISO/IEC is a general RA which describes the wider aspects of data privacy (Cyber risk countermeasures education, 2021, p. 52).

4. Method

The following chapter describes the methods used in this project. The section explains, evaluates and validates the approach of this study. It will also describe how relevant data was collected in order to be analysed.

4.1 Qualitative Data

Conducting interviews are considered to be a qualitative research method. A qualitative research method aims to give the reader an understanding for individuals and different situations. The main focus of this method is to target the participants of the research's actions and subjective opinions. What emphasizes the method is that the participants perspectives are presented in a fair way in connection to the collected material. This provides the method with trust. It is important that the result fit into the social context where it is being studied (Fossey, et al., 2002). The outcome of a qualitative study varies depending on who is performing the study. Since the collected material is interpreted by the author of the study the results are depending on the person's interpretation of the received information (Dalen, 2015).

4.2 Data Collection

In order to collect the data needed for this study, a combination of interviews and system analysis has been performed. Forsgren, Humble and Kim (2018) describes how this combination can be used in order to study software development. Data can be collected from both surveys as well as by observing digital systems. Forsgren et al (2018) describes how digital systems can explain a lot of things but the information is not meaningful without context which can be provided by employees handling the system. Therefore, measuring completely with one or the other is difficult since they provide a setting for both types of data. The disadvantages of these kinds of data are quite similar. This since it in both cases involve bad actors affecting the result. When it comes to system data there is nothing stopping people from tampering with the files and sabotaging the collected data. This applies to surveys as well since people can lie when answering survey questions and the responses might then have an effect on the result. Although, counter measures can be applied in order to avoid these kind of situations for both types of data (Forsgren, et al., 2018, p. kap. 14).

4.3 Interviews

4.3.1 Semi-Structured Interviews

Semi-structured interviews were chosen for this specific study since the questions asked are quite complex. The project deals with subjects connected to requirements and legislations which can be both advanced and complicated. According to Christensen,

Engdahl and Grääs (2010) this type of interview method is suitable for these kind of intricate questions. The method gives the opportunity of asking follow-up questions which hopefully could give a more thorough interview and more clear answers (Christensen, et al., 2010). In a study with several interviewees, a semi-structured interview is suitable to ensure a certain minimum of comparability between the interviews according to Bryman & Bell (2017).

Bryman and Bell (2017) explain that qualitative interviews are conducted to investigate what the candidates themselves find interesting and relevant (Bryman & Bell, 2017). This was considered valuable for the study since it will help getting a deeper understanding for how employees' reason when handling customers' personal data. Also this topic in relation to the roles described in the RA. With semi-structured interviews it is also not needed to handle the questions in set order (Christensen, et al., 2010). According to Dalen (2015) research proves that even though interviewees partly master the interviewers language participants should always be presented with a choice. There can be quite few that feel comfortable enough conducting a scientific interview in the relevant language. Therefore the interviewee should always be given the choice of language for the discussion (Dalen, 2015, p. 38).

4.3.2 Interview Guide

The surveys conducted in this study consist of interviews and more specifically, semi-structured interviews. In order to prepare these in the best way possible, interview templates were made. The purpose of the templates, explained by Bryman and Bell (2017) is to have a manuscript on what the interviews are based upon. For this study, it was decided to use a combination of fixed and spontaneous questions so that the possibility of further discussion was possible at all times. The questions covered topics such as the interviewees daily work, employment role, data handling, security and data ownership. The interview guide see Appendix B for English and C for Swedish, consisted of questions sorted into multiple topics that were to be discussed. According to Bryman and Bell (2017) there is always a general risk that interviewees could experience the questions as uncomfortable which might affect the result of the interviews. In order to avoid this, the purpose can be sent to the participants before the interview so that they get a chance to prepare themselves and also convey if any questions are overly sensitive (Lynham, 2002). According to Dalen (2015) an interview guide can be changed after tested during an interview. During discussions the interviewers can give useful reactions to how the questions have been formulated. This can lead to questions being reformulated, added or removed from the guide (Dalen, 2015, p. 40).

4.4 Discourse Analysis

Discourse analysis can be briefly described as a way to understand and study language use and its effects on society, people, and their relationships with one another. More

specifically, discourse analysis is a method for studying language use that can be suitable for a research or thesis projects. The method is useful for describing the role of language used in everyday life. In discourse analysis, language is not seen as an abstract system of rules but rather as an action. We perform actions when we use language, and language in turn influences the way we experience, think, see and feel (Svensson, 2019, p. 16). Discourse analysis can also be used to understand the descriptive role of language and give an understanding of the important role that language plays in people's experiences (Svensson, 2019, pp. 16-17). Discourse analysis as a method can be applied on multiple different ways of communication where interviews are one of these. If the dataset collected from interviews can be categorized according to topic, different discourses can be identified which later can be used for further discussion and evaluation (Börjesson & Palmblad, 2007, pp. 16-18). Discourse analysis therefore opens up for broad interpretation as well as a combination of information sources. When performing a discourse analysis on data collected from interviews it is important to remember that the researcher abandons the assumption that there is only one accurate interpretation of a participant's answers. This means that the result of a discourse analysis can be heavily affected by what type of researcher is performing the method (Talja, 1999).

An interview situation however, exists only as an effect of a research project, and it is therefore difficult to assess whether what the interviewee talks about during the interview is something the person would have said in other situations where the researcher is not present (Svensson, 2019, p. 103; 108; 115). When listening through the interview, notes should be made on possible themes, issues, observations and ideas. All themes and observations are potentially relevant, and it can be difficult to determine in advance what is interesting and what should be discarded, but it is better to give it the benefit of the doubt (Svensson, 2019, p. 121).

Another kind of discourse analysis is conversation analysis. This kind of analysis requires the researcher to take the context which is presented in the empirical material into account. In other words, the inner context, the one which is expressed in the studied conversation should be taken into account in the analysis in this case. This means that nothing mentioned in the conversation is being analyzed. So topics that address e.g. the past, gender, age, class and politics of the participant, should not be included as an explanatory variable in the conversation analysis. The conversation analyst should also analyze the empirical material as unbiased and open minded as possible. Another premise is that all details can turn out to be significant for the analysis. This means that the researcher should not omit anything from the material even if there are deviations from the patterns you may see in the collected material. Individual deviations can provide clues to different variations of the conversational rules that govern the interaction, such as hesitations and pauses. These small details are important for understanding how a conversation is organized and carried out by the participants, which is why it can be useful to record the conversation (Svensson, 2019, p. 73). In these cases, the researcher must transcribe the recording to create the empirical material that can then be analyzed. This is

important for several reasons, but one reason is that it is often easier to get an overview of empirical material when it has been written in text rather than when it is conveyed through speech. By formulating and asking questions to the interviewee, the researcher contributes to the development of a text in the interaction between interviewer and interviewee (Svensson, 2019, p. 103;108;115).

An analysis of the empirical material should first and foremost be based on the research questions formulated for the relevant project. The research questions simply constitute the questions to be asked of the empirical material, which can be important to consider when conducting an interview study, e.g.:

A workflow for performance of discourse analysis can be:

1) Familiarizing yourself with the collected material
2) Organizing the empirical material
3) Close reading
4) Thematization
5) Contextualization

The purpose of familiarizing oneself with the collected empirical material is to prepare for the analysis and to be able to analyze details in the text. The second step in the workflow is to organize your empirical material in a way that allows you to proceed with the analysis. The third listed step is close reading of the empirical material. When asking questions such as “what is happening here?” and the question should be asked for each new line or sentence in the transcribed text. The discourse analyst’s attention then shifts to language use and its social effects. The repetition of the question forces the discourse analyst to constantly return to what seems to be happening in the document or social interaction under study. Moreover, the question makes it possible to interpret and not just describe the text (Svensson, 2019, pp. 133-140).

The fourth step in the process is thematization, which means that themes are created according to what best summarizes what has been discovered in the empirical material. The main reason for doing thematization is to determine what has emerged from the close reading so that the information can answer the research questions. Thematization is done by categorizing the results of the close reading based on similarities and differences. A category consists of empirical findings that are similar to the research questions and it should also differ from these. In practice, it is difficult to avoid overlapping categories, but the ambition should be to maximize both the differences between categories and the similarities within a category (Svensson, 2019, pp. 142-145).

The fifth and final step in the process is contextualization which involves studying the empirical material in a broader context such as social, political or historical contexts. The analyzed text is placed back in the context from which it came. This opens up the possibility of understanding the role and function of language, which allows us to e.g.

understand the decisions and actions of a workplace. For the critical discourse analyst, contextualization becomes a question of identifying the context that is not immediately visible in the empirical material. Contextualization does not necessarily involve either identifying or imposing a context, but rather anchoring a context to the analyzed text (Svensson, 2019, pp. 145-149).

4.5 Validity and Reliability

When it comes to interviews, the questions regarding whether the results obtained are reliable or not should be discussed. Validity answers the question whether the method is considered reliable and answers the questions asked in the study. A study is said to be valid if the result answers the questions asked and the purpose of the investigation is fulfilled. When a study is based on interviews, the question of bias has to be raised. An interview only gives one person's perspective and the answer might be based upon their own personal experience. In other words, it might only provide you with one perspective. In order to avoid confusion and strengthen the reliability of the study, all interviews were recorded. This way it was possible to listen to the interview again and sort out any uncertainties and control answers. The notes taken during the interviews also helped with this (Kvale, et al., 2014). It is important to reflect on the researcher's role in performing a study with this kind of method. Since the result can be heavily influenced by this person's perception of the collected information the conclusions have to be evaluated. In a semi-structured interview, the researcher listens to an interviewee's answers which gives room for interpretation. Interpretating information conveyed in written text is easier than when it is communicated through speech. Therefore the role of the researchers has to be reflected on and assess on to what extent their perspective could influence the analysis (Dalen, 2015).

Regarding discourse analysis as a method, similar issues might surface as the ones discussed when it comes to interviews. The so called "bias-problem" is defined as: "en snedvridning av forskningsresultat på grund av systematiska procedurfel i urval, insamling och analys" [a distortion of research results based on systematic procedural errors in selection, collection and analysis]. This means that a study could risk turning out biased if the researcher has done consistent misalignments throughout the project (Börjesson & Palmblad, 2007, p. 19). It is also important to remember as a discourse analysist that when performing the method, the researcher is not an observer of the relevant discourses. In order to observe and analyze a discourse, the researcher has to participate in the discussion. The performed research is therefore both a product and a producer of the discourse. Qualitative research can be demanding of the researcher since experiences and knowledge play a big role (Bolander & Frejes, 2015).

Confidentiality in research refers to the agreements that participants enter into and usually means that private data identifying the participants in the survey will not be disclosed. If you are going to publish information in a survey that could potentially be recognized by

others, respondents should agree to the release of this identifiable information. In studies with individual interviews, it should be clear before the interview begins who will later have access to the material. Anonymity should protect participants but provide the necessary specific information required for other researchers to repeat the study (Kvale, et al., 2014, p. 109).

5. Methodology

In the following sections the implementation of the chosen methods is presented as well as the way of work. The collected data will be evaluated and reviewed. The chapter also describes the way of working with the study and how the theoretical framework has been applied to the approach.

5.1 Applying the Reference Architecture

When starting to analyze the decided RA, a few aspects were taken into consideration. It was discovered after studying the organization, through the first interviews and through discussion with our supervisor at YIAS, that some roles would not be relevant for the studied case. As described in section 3.1, an already existing RA can be modified in order to suit an organization better. This is usually done through, removing, replacing or altering responsibility roles described in the theoretical RA which in this case is the standard. Therefore the standard has been modified in order to suit the YIAS department's needs and structure better.

According to multiple interviewees, the YIAS department has so far not been working according to a set RA. As a result of this, it sometimes happens that groups work in so called silos and not comprehensively across the department. The expression "working in silos" explains the fact that many employees do not communicate as wished with other groups. This can sometimes create misunderstandings and make it difficult to get a clear picture of different groups progress. Since the methodology is missing a blueprint, this can make it complicated for groups to work together and see the overall picture. When starting new projects, an extensive amount of time is sometimes put on mapping the cloud architecture since some parts have been built individually and not according to a reference. Therefore, the need for a suitable RA for cloud computing within the department is sought after.

Continuing on the first paragraph in this chapter, it will now be described how the RA was modified. Since YIAS only uses Microsoft Azure as a cloud service provider no other supplier would be relevant for this study. Therefore the roles regarding *Peer provider (CSP)* were eliminated from the final RA. These were *CSP: service manager*, *CSP: operations manager* and *CSP: business manager*. Since it could be stated from the beginning that these roles do not exist within YIAS and therefore never would be relevant for the studied system nor the department. For the same reason the *CSP: inter-cloud provider* was removed from the RA since this role is also reliant on multiple cloud service providers.

It was also decided that the *CSN: broker* was to be removed from the framework. As described in section 3.2, the main tasks of this role are relevant before the contract between the company and cloud service provider has been made. This was also

considered a non-relevant role for the study since the business between Vattenfall and Microsoft had already been settled when the project started. Vattenfall has used Microsoft Azure as a cloud service for years so this role has not been relevant for a long time. Therefore it was removed from the RA framework.

After these modifications were made, the final RA can be viewed in Figure 3. Here, the relevant roles have been sorted in departments according to business area.

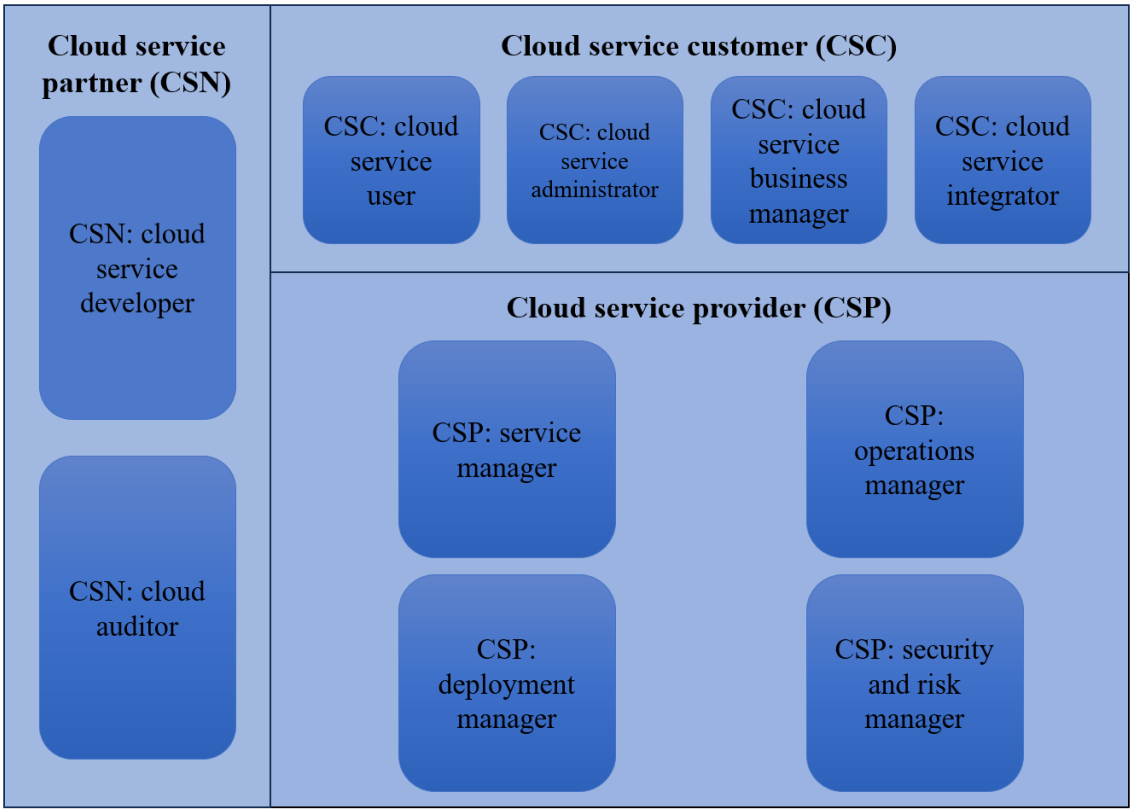

Figure 3. The ISO/IEC 17789 RA with modifications.

5.2 Interviews

During the project, multiple semi-structured interviews were also done with our supervisor at the department. The main data collection however was done through 22 semi-structured interviews with employees within the YIAS organisation or in close cooperation to the department. The interviewees were asked to spare one hour for the interviews but the meetings were sometimes shorter or longer. The interviews focused on how employees reason when handling personal data within the cloud environment as well as more organizational topics such as company structure. The interviews also focused on the responsibility roles presented in section 3.2.2 that are described in the RA. This in order to determine if all these roles exist and if one was missing why that is the case. The interviews also helped to get a clear picture of how data flows within the department.

As mentioned by Bryman and Bell (2017) and discussed in section 4.3.1, there is always a risk that an interviewee might feel uncomfortable when being asked questions. In order to avoid this, an e-mail was sent to the interviewee beforehand with topic questions and a brief overview of what the interview was going to be about. The interviews were also conducted in a secluded room so the conversation could be held in private. Before booking interview slots with relevant employees, the interview guide had to be made. The interview guide was designed in order to cover all the relevant topics for the project. As described in section 4.3.2, each interviewee was given the opportunity to choose language for the discussion. This lead to the interviews being conducted in both Swedish and English. Therefore a separate guide was made for each language. These guides were thoroughly processed and well managed. The two guides can be viewed in Appendix B and C. After two interviews had been conducted it was decided that the interview guide had to be changed. This was done to avoid repetitive questions and to get clearer answers. Two questions were also added in order to make the process easier in knowing if the questions belonging to blue, green or orange should be asked, see Appendix B or C. When it was time to schedule interviews all employees considered relevant for the project were contacted. Some interviewees we had previous contact with and some people were new to us. Our supervisor at YIAS also helped with getting in contact with a few employees and introducing us to these.

A semi-structured interview was concluded to be a suitable interview method for collecting information. Since the questions asked were related to topics that were normally not that heavily discussed among the employees. Many interviewees also stated that the questions concerned areas they had not reflected on or discussed in that context. In Appendix A, Table 3 is attached which provides an overview of all employees interviewed for this project.

5.3 Introducing the Environment

Interviewee No1 explains that the digital systems that are being studied belongs to and are managed by *Customer IT Nordic's (SE/FI)*. This digital platform serves both internal as well as external users so it reaches a broad target audience every day. The environment consists of three main parts called Governance, Microsoft Azure and *Data Center (DC)*. The internal users utilize the environment primarily for reporting. It consists of *Customer service (CS), Business to consumer (B2C)*[18] and also serve eMobility with analytics and also *Business to business (B2B)*[19]. EMobility is the system which manages customer matters related to electrification of means of transport such as electrified cars (Vattenfall Customer IT, 2023). External users mostly use the

[18] B2C is an abbreviation of Business to consumer (House of IT, 2021).
[19] B2B is an abbreviation of Business to business (House of IT, 2021).

environment to access the energy site and energy business portal. This is done through external business partners like e.g. *B2B Heat*[20].

The second part of the environment contains a cloud in Microsoft Azure. This cloud has three different parts that will be described in the following sentences. In the cloud, the main part is made up by the YIAS department who's main focus is to deliver customer experiences through digital platforms together with the relevant business partners. The main business partners of YIAS are Customer Solutions Nordics (including B2B Sales, B2C Sales, Commodities), Customer Service Nordic, Customer facing solutions for Heat SE and Distribution SE. Within YIAS there are also three different teams where one team is working in *Complex Event Processing (CEP*) within frontend, according to interviewee No1. The second part of the cloud regards Integration where *Vattenfall Integration Platform (VIP)*[21] can be found. VIP is a complex hybrid integration platform which works with Microsoft Azure and on-premise infrastructure, as well as general technologies, governance, rules, guidelines, and security (Pönisch, 2023). The third and final part of the cloud is *Vattenfall Analytics Platform (VAP)*[22]. This part provides support within analytics to the customer related parts of Vattenfall Nordics. This includes both technical and strategic advice as well as building platforms and solutions to enable analytics within the business. Together, these three components constitute YIAS (Vattenfall Customer IT, 2023).

The third part in the environment is a data center and the main function of the center is to process orders, modifications and decommissions of server and their components and connect the requester and the operational team (Kochanek, 2022). Within the data center there is both a backend and an integrated part that delivers data to both external and internal users. Together, these three parts form the cloud environment that the project will evaluate.

At Vattenfall, a *group governance framework (VMS)* is being used. The main function of the VMS is to form an internal part of the overall framework which is closely aligned to other business units and staff functions to deliver consistency across the Vattenfall group. The VMS reflects that Vattenfall is subject to many regulations governing the protection of confidential information, financial accountability and service availability, among others. Vattenfall also needs to comply by the requirements and wishes of its shareholders, external stakeholders and customers. In this context, the Vattenfall IT Governance provides a framework of best practices and controls that helps ensure that its deliveries meet both internal and external requirements (Lindqvist, 2022).

[20] B2B Heat is an "all-in-one platform" enabling customers to control their energy consumption (Vattenfall, 2023).
[21] VIP is an internal name for Vattenfall Integration Platform (Vattenfall Customer IT, 2023).
[22] VAP is an internal name for Vattenfall Analytics Platform (Vattenfall Customer IT, 2023).

5.4 Data Handling by Discourse Analysis

In order to get an overall view of the information collected from the interviews the data was thoroughly processed. As mentioned in section 4.4, a risk with semi-structured interviews is that spoken information can be interpreted in different ways by different people. To make sure that the researchers interpreted the answers from the interviews the same way, the information received was discussed after each meeting. This way we could reassure ourselves that we had interpreted the information in the same way which strengthened the reliability of the method. Interpretation of the material is also a problem which can occur when performing a discourse analysis. To make sure the our own understanding would not affect the results and discussion, a continuous dialogue regarding the data was held between both researchers. This would also make sure that the data was interpreted in the same way. In the following sections 5.4.1-5.4.3 the reasoning behind what role was given to what interviewee is described. By analysing the data collected from interviews it could be determined which role was suitable for each person. This was done through discussing the answers and comparing them to one another in order to determine which role was fitting for each person's responsibilities and daily working tasks.

5.4.1 CSC: Cloud Service Customer

When putting people in the section of CSC, the first reason for doing this was that these employees interact with the cloud services as users, not as developers. The second reason is that each employee put in this section in one way or another has a relationship with the business departments of Vattenfall. This is an indication for an interviewee to be part of the CSC. Since the following paragraphs only describes roles within the CSC, all mentioned roles are part of this section. In section 3.2.1 it is described how a role within the CSC uses cloud services in their everyday work life but is not responsible for the development of these. No11 describes their working role as: "making sure that the processes are there and are updated but I do not do the updates". This indicates the employee manages cloud services and use them but is not involved in the development or updating of the systems. Similar answers were given by interviewees No16, No17, No18 and No20, also placed in the CSC part of the RA. Starting with No18 who is put as the role of a *User*. This interviewee designs front end solutions for the end-users to make them suitable for the relevant customers. This means that No18 does not use cloud services themselves but rather designs other systems used in connection to such digital services. In order to do this, No18 has a close business relation to the departments responsible for making sure that the systems available to the end-users fulfill the right needs.

Moving on to No20 and No17 who are both defined as the *Administrators*. Since this particular role is mainly responsibility is to make sure that the cloud services are well-functioning for the end-users. This employee monitors the entire process but is not

involved themselves in the development but rather the design of the digital system. This became very clear when interviewee No20 was asked about their work with deployment of cloud services. No20 explained that they do not develop the services, instead: “we design them and do not work with them. We make a design which the other teams can access and use”. No17 gave similar answers which made them both suitable for the given position. So, No20 and No17 has a similar function as No18 when it comes to designing digital systems, but the Administrator has more of a managing responsibility when it comes to design. This is the biggest difference between the, in this paragraph mentioned responsibility roles.

When looking at the position *Business Manager*, interviewee No11 was suitable. No11 describes their role as a managing role where they are responsible of the smooth operations of multiple different applications. They also explain how they have a responsibility to make sure the applications are working as expected but also running cost-efficiently. It is explained in the RA that this specific role makes sure that the services available for the end-users are meeting business objectives and saves as much resources as possible. This employee does not interact directly with the systems but makes sure they are living up to the business objectives, which No11 describes they are doing in their daily work. This is done through e.g. continuous meetings with scrum masters in the team. Therefore it was concluded that No11 fit the role of a Business Manager.

Moving on to the last part of the CSC which is the *Integrator*. The main responsibility of this interviewee is to make sure the integration of the cloud services within the company are running smoothly. This employee also work with the overall customer experience within the systems available for the end users. Interviewee No16 describes a main responsibility in their working role as setting up the data strategy and rolling out implementations for future integrations. This falls into the responsibilities of an Integrator since this employee makes sure the implementations are well thought through and also improve the end user experience. Since No16 also mention that they work close to the Vattenfall business departments which further strengthens the argumentation that No16 is part of the CSC responsibility roles.

5.4.2 CSP: Cloud Service Provider

The roles within CSP work with making cloud services available to other cloud service customers. All CSP roles require focusing on the cloud computing activities necessary to ensure its delivery to the cloud service customer, as well as cloud service maintenance. For a person to have a role within CSP, they are also responsible for the relationship with the business. In general, CSP roles have technical tasks and at Vattenfall these tasks and roles are linked to at least one of Vattenfall’s technical platforms, systems or processes. Based on the interviews, we have identified six people No9, No10. No12, No13, No14 and No22 who fit into one of the roles listed under CSP. Since the following paragraphs only describes roles within the CSP, all mentioned roles are within this section.

From the interviews there are two people No9 and No12 who both fit best under the role of a *Service Manager*. No9 explains that it works in an overall role where the person ensures that the processes are running smoothly. To belong to the role, you need to ensure that the functionality works and also that you meet the requirements, which No9 describes that the person does in their work. No12 works with several of Vattenfall's technical services. No12 says that the tasks are about developing activities to make the cloud services available, which fits well with the description of what a Service Manager works with. No12 explains that you always have a business relation and that it is a must because it is not possible to work in silos but you have to work together IT and business. No12 explains what the relationship looks like through an example. In the example, someone from IT wants to implement some new rules for a system that business is working on. This means that this person has to tell the stakeholders what they need to implement that functionality to get the right security point of view. It is therefore important to make sure that business also understands what you want to do, why, and that it is important for their work as well. This description fits well as an example of how a Service Manager works.

No10 works with products that are presented to end users in terms of performance, security aspect of it or any aspect of reliability of specific system which means that this person fits well under CSP. We have decided that No10 was chosen for the role of an *Operations Manager* as the person's tasks are mainly about simplifying processes for developers. No10's main task is to understand how the existing process works and which areas can be improved within the technical department and then allocate tasks to developers. Moving on to No13 that we decided belongs to the role of *Security and Risk Manager*. No13 works closely the business and giving support in helping the business comply with the regulations hence it is clear that the person belongs to CSP. The main responsibility in this role is to ensure that the cloud service provider manages the risks associated with the cloud services. One of No13's daily tasks is to ensure that Vattenfall is compliant and that the information security policy is appropriate, which are exactly the tasks that describe that position. Similarly to No13, No22 also works together with the business with a large responsibility for security and risk management. Daily tasks for No22 includes providing the organization with recommendations for information security as well as support during risk assessment. Educating other staff is also relevant on a daily basis for No22. This means that No22 acts like a support when it comes to development and delivery of cloud services. Since this employee does has a responsibility regarding risk and security and a close business relationship, it was decided that No22 would fit the role of a Security and Risk Manager.

Moving forward we have also analyzed that No14 belongs to CSP since the role is involved in planning the deployment of a service into production which makes the person belong to the *Deployment Manager*. The work is overall and ensures that the teams handle the daily tasks. No14 is involved in the step where the technical solution is approved, which corresponds to the role described as managing the initial steps and dependencies for deployment and activation of operations processes used.

5.4.3 CSN: Cloud Service Partner

To be able to belong within the CSN the person has to support and assist the activities conducted by both the CSP and CSC. At Vattenfall we have identified that the people working within CSN mostly has a role that is connected to both parts. Within CSN there is four people from the interviews that belong to two of the CSN roles and these are No8, No15, No19, No21. Since the following paragraphs only describes roles within the CSN, all mentioned roles are within this section.

The first reason for placing people in the role of *Developer* was that the main responsibility of these employees is to design and develop the implementation of a cloud service. We have identified three people: No8, No15 and No19 that all work with these tasks. No8 describes that the job is about trying to find the best technology and ensuring that the company then implements that solution. As a Developer, you also work on testing and maintaining the implementation of a cloud service. No8 says that as part of their work, they test to ensure that the system meets the requirements that are defined. As the work itself is technical is also includes administration of the technical tasks, which is consistent with the CSN section. No15 describes the tasks as design of various integrations within projects that are all related to the cloud, which means that the role Developer fits well. Another reason why we chose this role is because No15 described that the work is with data from both IT and business. No19 describes their daily work as similar to No8 and No15. No19 describes their work tasks mainly as development of cloud services and security controls of the these updates. Therefore No19 also fits the description of the role as a Developer.

Within the CSN section, there is also a role called *Auditor*. The main task of this role is to be responsible for conducting an audit of the provision and use of cloud services. No21 fit into the Auditor role. No21 works with the audit and provision of the system and also ensures that the installation takes place. This description of the role is consistent with the description of an *Auditor* as the work of the role is to audit cloud services and often includes operations, performance and security and investigates whether a certain set of audit criteria are met. No21 described their main working tasks in the interview as a mix of security, governance and deep technical issues. To be able to say that No21 is also part of CSN's audit, the person should be responsible for conducting an audit of the provision and use of cloud services. We believe that the employee does perform this when they explained that they work with managing the governance within the cloud as well as setting up security levels and infrastructure. Therefore, it is clear that No21 has the role of Auditor.

5.5 Data Ownership

In order to determine ownership of customers' personal data, categorization in accordance to discourse analysis was done, see section 4.4. In the interview guide we had a few

questions about the ownership of customers' personal data. In order to do this, three different categories were constructed. Also, since some of the interviews were held through Microsoft Teams we were able to record the meetings and use the transcript function that automatically generates the interview transcript. We followed the five steps of discourse analysis so we started with familiarizing ourselves with the collected material. This was done by continuous discussions after every interview as well as going through notes. To be able to focus on data ownership we sorted out the questions that regarded this topic. That made it easier to see if we needed more information or if the information we had collected helped us to state the ownership. With help from both our notes and the autogenerated transcription, it was possible to analyse the answers. The answers we sorted chose to focus more on we then analysed in more depth by close reading. The answers given from the interviewees were then categorized according to these topics to sort out the, for this research question, relevant information. The data collected from interviews was sorted on these categories in order to make sure relevant information was being used in the analysis.

Category 1: Statements indicating a clear data ownership.

In the first category, the interviewees describe a clear ownership of customers' personal data. It was concluded that a total of four people could be categorized to this category.

Interviewees placed in this category stated that the ownership within the organization can be stated as clear. These employees could describe who they considered was the owner as well as why they believed so. A number of different working roles were stated as owners and it was described how they help to ensure that security requirements are met and regulations are being followed. Having this knowledge makes it easier for employees to know who is responsible which then helps if uncertainties are to emerge. Another conclusion that was drawn from this category was that interviewees are aware of each employee's own responsibility regarding the matter. This is conveyed through different courses and meetings about the topic which interviewees consider being helpful reminders of their responsibility. A general opinion in this category was that people find the ownership clear, however there is always room for improvement. Interviewees find that such an improvement could be that customers' personal data was to be stored with a better structure within the company. It would be easier if these types of data were not stored within each group or department but instead were accessible from one source to all parts of the company that needs to handle it. An interviewee in category one describes it as "customer data is stored in silos depending on who owns the data and it could be more transparent" […] "this limits the potential of sharing data". This brings us back to the user case described in section 2.1.1, which is an example mentioned by multiple interviewees in this category. Making sure that this user case can be handled correctly is an improvement the majority wants to see.

When we analyse the answers in this category, it is clear that all interviewees believe that they know who is the owner of customers' personal data. This conclusion is particularly interesting since from the analysis, the participants do not state the same working role or person. This means that there are different employees and different working roles that the interviewees consider to be the owner of customers' personal data. It can also be concluded that people have a generally good impression of the courses that are available on the matter and find them to be a good reminder. This is good input since maybe this could help state the ownership more clearly.

Category 2: Statements indicating a not very clear data ownership.

When we were familiarised with the collected empirical material we saw during our analysis, statements that indicated a not very clear data ownership. This category was for the employees that did not exactly know who the data owner is but indicated knowledge about who they suspected was the owner. The majority of the participants in the interview study belongs to this category, seven interviewees.

A consistent opinion in category two is that the ownership is quite unclear and therefore there is room for improvement. A few interviewees mention the business side of Vattenfall as being the owner but most participants could not further explain or name these working roles or employees. One participant in this category stated that "I am wondering if customer IT even owns any personal data. It belongs more to business. It should be clearer and better stated, all responsibilities should be described more clearly". Many interviewees mention a knowledge gap within the organization regarding the matter. By gap, interviewees mean the roles and responsibilities of different information owners and system owners which is stated by a majority in category two. This is situation is described as "we have a gap between different owners and in all cases we have search and understanding but when you go inside the business, the ownership is not very clear". So in some cases there is a lack of understanding regarding information ownership.

People in this category also state that it is mainly connected to system owner responsibilities that are described as somewhat confusing at times. The idea of process owners is also mentioned as something that might make the process more clear and more specifically, process owners connected to GDPR. It is suggested by interviewees that this employee should focus on GDPR since they then would be familiar with the deletion of data since it is a fundamental part of the legislations. If there could be a person stated as responsible for the process that is being wished for, it would make the ownership of data easier. The process in this case could e.g. be a digital system which handles customers' personal data and if you were to have a person responsible for this GDPR process you also have an employee who owns the data. Suppose that the situation describes in the user case (section 2.1.1) was to occur. If there was a process owner put in place for this action, it might be easier to track the deletion. This process owner would also be required to have good insight in GDPR related questions. If an employee was to be responsible for the

whole activity chain it would most likely be easier to find and delete all the correct data. Process owners are mentioned by multiple employees as a possible solution to the challenge. Interviewees also mention the mandatory education on the topic as important, just like category one. However, it was also stated that if data is available in several systems, this builds complexity. Therefore there are times when the owner is not completely obvious because ownership is moved around which can be confusing at times.

In conclusion, most interviewees in category two consider the business side of Vattenfall as well as the system owners to be the owners of customers' personal data. However, people mention a knowledge gap which makes it difficult to know the exact owner is. In this category there are indications as to employees having the impression that Vattenfall might not even have a data owner. The main impression is that it should be mentioned in each project who is the data owner is for that specific case and the specific types of data that are being used. Employees are under the impression that this would make the information easier to find as well as more specific since it would be connected to processes.

Category 3: Statements indicating an unclear data ownership.

The people in category three had trouble answering the question if they could clearly say who the data owner is. In conclusion, these interviewees were under the impression that the ownership of customers' personal data is not stated clearly within the organization.

In general, the interviewees placed in category three consider each employee as responsible for customers' personal data. However, many stated that they say this because they are not sure who the owner actually is and find it difficult to find out. Most people do not believe it is one specific person but rather the organization as a whole. It is considered to be a difficult topic to understand and many state that the question does not really have a clear answer. When one interviewee in this category was asked the question regarding what responsibilities they have as an employee regarding customers' personal data, the answer was "that is exactly the part we are missing today, who should do what". Interviewees also used the user case described in 2.1.1 as an example to describe the problem. If we have different systems with personal data, and one customer decides or request that they want to remove their data it is a complicated process since data has to be removed in all systems where it is being used. Someone has to make sure data is removed from every source and the process for doing this is unclear. It is possible to remove data from one specific system but if it really covers everything the customer wants to have removed it is hard to be certain. In this case, it was stated that finding the right person who owns the system who also knows how to handle such a question is hard. In order to solve this, awareness was described as a main part. If employees are aware of how the company is supposed to handle customers' personal data, then the processes will be easier as well. As an interviewee stated, the company does not have a clear data owner today so "we need to make an organizational change to make the ownership more clear".

When analysing what the people in category three stated, it can be concluded that the interviewees seem to be aware of the fact that there is an issue. The ownership is not clear at times and it is something that needs to be stated more clearly so that it is obvious who to contact when questions emerge. To get a clearer picture of how the participants in the interview study found the ownership of customers' personal data within the organization, a diagram was conducted. The diagram is pictured in Figure 4 and shows where each interviewee is placed regarding how clear they found the ownership of these types of data.

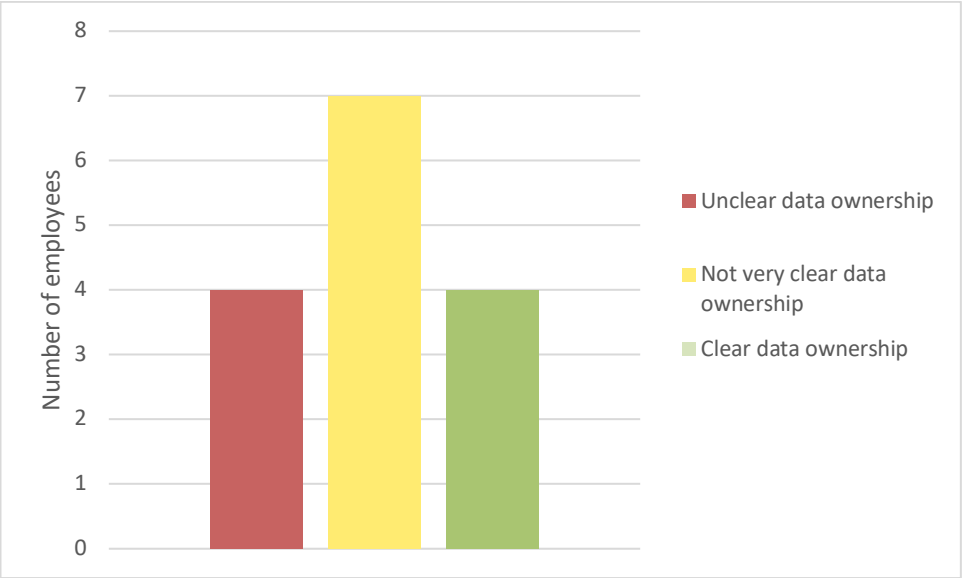

Figure 4. A diagram which shows how the clear the interviewees find the ownership of customers' personal data.

5.5.1 Data Breach

During the discourse analysis for data ownership we also found answers related to data breach. Since we got answers concerning the fact that the ownership of data was not clear for all employees we decided to add one question to the interview guide, see Appendix A and C. We wanted to ask the participants about their knowledge regarding what they and the organization should do if there is a data breach. Since some interviews had already been held at the time we reached out to these people again, a short call or message via Microsoft Teams was sent out in order to get the information needed. The main reason we decided to add the question about what happens if there is a data breach was because we also wanted to investigate if there was a connection between peoples' knowledge about data ownership and data breach.

In general, the majority of participants in the interviews have a not very clear understanding of what happens if there is a data breach within the organization. Vattenfall has a process in place and a reporting structure that is clear. The employees that understand what they should do and the organization should do if there is a data breach states that it is important to take immediate action in order to isolate and contain the

breach. This may include disconnecting affected systems, restricting network access or temporarily disabling certain services. If a data breach is detected, you have to inform relevant people about the situation. If there is a significant incident, the first thing you do is that the situation has to be contained so that it cannot spread and get more severe. Relevant affected parties has to be informed about the breach so that the incident can be taken care of as fast as possible. As well as contact the authorities if there is a leakage of personal data. Both internal and external stakeholders has to be informed about the breach, including what steps the organization is taking to address it. Although, when an incident occurs, business and IT work together to solve the situation. And a few people state that there has never been an incident like this but they do know how to handle the situation if a data breach was to occur and what processes apply.

Although the process was clear for the majority, there were some improvements that employees mentioned that could make the handling of a data breach even better. One of the improvements was that the organization should conduct a throughout analysis of the breach to identify the root cause and any vulnerabilities in the systems. Including revive and update security polices and monitor audit so that you regularly monitor and audit your organization's systems and processes to identify potential vulnerabilities.

There is a growing interest among employees to both understand and explore how the process works so that they know what to do and feel secure in the steps. Especially since employees have not been trained or have performed any fire drills regarding data security incidents. Interviewees who have a not very clear understanding of what to do when a data breach is detected stated that the emergency number that should be called is hard to find. Also, who to contact next after this phone call is unclear to multiple employees. Today, many fire drills are done in order to practice what happens when there is a physical fire. However, when it comes to a data breach, no similar practice has been done. Interviewees state that this is something they believe would be beneficial for the organization, announce and update all employees, system managers and colleagues on what to do in the event of various security threats. People who find the process unclear explains that the structure of the processes has to be improved. One interviewee described it as "if something happens tomorrow, I do not know what actions would be made but I know who to call". This is a problem with large organizations, there are too many stakeholders at times which makes it hard to know what employees should do when something happens. Some interviewees stated that if they were to leave the organization, they would not know how to ensure that their replacement would receive this knowledge since you mainly gain it from experience. Since the frequency of new employees is high, a virtual emergency drill is just as important as a physical one. This is important since some interviewees stated that they do not really have knowledge of what would happen if a data breach was to occur. E.g. an interviewee said when asked what to do if there is a data breach "I have no idea. What will happen is not clear however we know it is very important" [..] "what can happen in a real case is not clear, but I believe it would be very serious".

In conclusion, Vattenfall's different systems are secure and employees have great trust in these. However, if a data breach was to occur, the most important and first thing to do is to alert the people responsible. The majority of the interviewed employees has a clear understanding of what happens if there is a data breach within the organization. Although, not all employees consider the process as clear and the main problem seems to be understanding about the process. Employees themselves ask for more information about the process and regulatory virtual emergency drills to increase their knowledge and to make them more confident in case of an emergency. One improvement is also that the organization should conduct a throughout analysis of the breach to identify the root cause as well as any vulnerabilities in the systems. It is clear that all employees consider a data breach as a relevant topic and an important aspect hence a data leak could harm both Vattenfall's image and customers' trust. The increased interest could be a result of the increased number of cyber-attacks targeted towards the organization.

6. Results

In order to answer the two research questions: How can a cloud environment architecture be organized in order to handle personal data? and What actions can increase the security of personal data in the cloud environment within YIAS? The following section consists of analysed interview data. The interview data was applied to the RA which shows the potential gaps between the current structure and the theoretical one.

6.1 Overview of the Current Handling of Personal Data

6.1.1 Results from Discourse Analysis

Since the discourse analysis was done separately by each of us, the interviewees were in some cases not given the same role. This provided the discussion with additional depth. Why were some employees placed in different roles? Since the main goal when performing a discourse analysis is to be completely unbiased as a researcher. The fact that we reasoned differently regarding some roles was interesting to investigate further. Had we interpreted the information from the interviews differently or were there other indications that lead to us placing employees in different responsibility roles of the RA. The resulting placement of interviewees can be viewed in Table 1. In this table, each interviewee is presented along with the given responsibility role as well as a potential alternative role. The alternative role came from us either placing the employees in different roles or when we found it difficult to place a person in an obvious role.

Table 1. A compilation of the results from the discourse analysis. The table shows each interviewee, their responsibility role as well as possible alternative role marked in italics. In this study 22 interviews (Appendix A) were conducted but interview no 8-22 focused on determining responsibility roles.

Interviewee	Responsibility role	Alternative responsibility role
No8: Developer	CSN: Developer	
No9: System architect	CSP: Manager	
No10: System architect	CSP: Operations Manager	*CSP: Security and Risk Manager*
No11: Manager	CSC: Business Manager	
No12: Developer	CSP: Service Manager	
No13: Security and risk	CSP: Security and Risk Manager	
No14: Manager	CSP: Deployment Manager	
No15: Solution architect	CSN: Developer	
No16: Developer	CSC: Integrator	
No17: Manager	CSC: Business Manager	*CSC: Administrator*
No18: Developer	CSC: User	
No19: Developer	CSN: Developer	*CSN: Auditor*
No20: Manager	CSC: Administration	
No21: Manager	CSN: Auditor	
No22: Security and risk	CSP: Security and Risk Manager	*CSC: Business Manager*

As shown in Table 1, four employees were not obvious as to what role they belonged to. Starting with No10 that was given the role of a CSP: Operations Manager with an alternative role of CSP: Security and Risk Manager. So that No10 belongs in the section of CSP was clear, it was rather the responsibility role that was not as obvious. We felt that No10 might also be suitable for the role as a Security and Risk Manager since No10 said that security and risk is a top priority for their daily work life. However, we ultimately did not choose that role as the employee stated that a main part of their work concerns cost optimization and performance. No10 describes it as: “I also look at cost optimization

and performance, however, security is consistent within my work". These are tasks that are more suitable for the role as an Operations Manager.

Moving on to No17 who was chosen for the role of a CSC: Business Manager but also relevant for the role of a CSC: Administrator. Similarly to No10 who was also relevant for a specific section, No17 was also obvious for the CSC. No17 has a managing role and is primary responsible for cloud-services smooth operation. The main reason as to why No17 was not given the role of a CSC: Administrator was that this one does not include a managing position. Both positions No17 was relevant for includes monitoring cloud operations and cloud based systems so that they are working as expected for the end-users. However, since No17 is in a supervising position it was decided that they were more relevant for the role of a CSC: Business Manager.

Thirdly, we have No19 who was considered for the position as a CSN: Auditor but was ultimately chosen for the CSN: Developer role. No19 mentions working with the audit and provision of cloud based systems as well as ensuring that correct installation takes place. However, No19's main tasks include development, deployment and updating of cloud based systems. Since these are described as main tasks and audit was explained as temporary tasks that emerge from time to time, No19 was given the role of a CSN: Developer.

Lastly, we have interviewee No22 who was given the role of a CSP: Security and Risk Manager but was also considered for the role of a CSC: Business Manager. No22 proved difficult to place in a specific working area which is proved by the two roles considered being in separate sections – CSP and CSC. One of the main reasons No22 was placed in the CSP was that they work closely with the business side of Vattenfall. Since this is one of the characteristics of the CSP, it was more obvious than the CSC. When it comes to working roles and responsibilities, No22 mentions that they specifically work with risk and security related questions in their daily work life. The role of a CSC: Business Manager does include many financial and legal aspects which No22 does not mention working with. No22 focuses more on the monitoring of cloud based systems so that they are compatible with Vattenfall specific risk and security regulations as well as managing a bigger group of employees. Since they also work with educating personnel on the topic, which is also described as a responsibility for the CSP: Security and Risk Manager, this was considered to be the more suitable role.

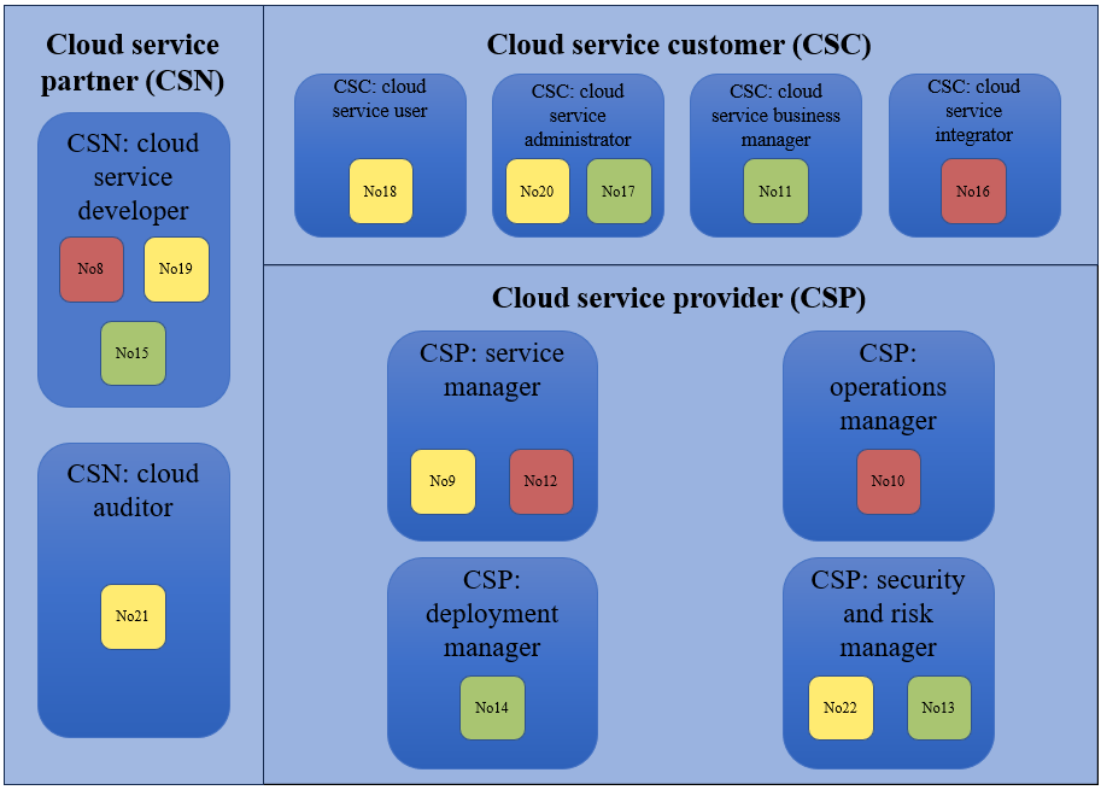

Figure 5. The final RA with assigned responsibility roles that has been color-coded according to Figure 4. This shows, for each employee, the perception of how clear the ownership of personal data within the organization is.

Figure 5 shows the final RA with assigned responsibility roles. Each responsibility role has an assigned employee according to the standard which means that the delta is small. Looking at both Figure 4 and 5, we found that the interviewees mainly found the ownership of personal data as not very clear. The number of participants that found the ownership unclear respectively clear were the same. This gives an indication of the employees' perception of the topic. In section 5.5, the three colour categories are described and this concludes that most interviewees are yellow and hence belongs to category two – statements indicating a not very clear ownership. Interviewees placed in this category expressed some sort of knowledge of the ownership as well as uncertainty about the topic. However, we cannot see a correlation between employees' perception of personal data ownership and the RA. The participants are evenly spread out and the study has managed to place an employee as responsible for each role. E.g., say that all employees placed in the CSP found the ownership of personal data within the organization as perfectly clear whilst employees placed in the CSN did not. If this was the case, it would have been interesting to investigate why this result emerged but since there is no obvious correlation the study can conclude that the topics do not correspond to eachother.

6.2 Suggested Solution for Handling Personal Data

Generally it is important to note that it is beneficial for the organization to act upon these findings. However, this does not mean that the data handling today within the organization is negligent in any way. This only means that the data handling and the recommendations surrounding it can become even better than it is now.

Based on the interviews, we can identify a need for clearer responsibilities and regulations regarding customers' personal data. As mentioned in section 5.5, multiple interviewees suggested and expressed a need for process owners in connection to GDPR legislations. Especially many interviewees mentioned process owners in category two which contains the participants who found the ownership of personal data as not very clear. Many thought that process owners would make the ownership more clear within the organization since it would make it easier to track it to specific projects and activity chains, if there was a process owner in place. If this person could be the one owning the personal data it would be easier to see where it is being used as well as finding the right person to contact if questions emerge. Further, when comparing these impressions to what is stated regarding ownership of personal data within cloud based systems, stated in section 3.2.3, there are similarities. According to the RA, the CSC supposedly should be the owner of personal data. Since the majority of legal requirements and legislations sit with the CSC section of the RA, it is recommended that the ownership should be given to one of the responsibility roles within this section. Putting together these two concepts, the recommendation might be to put the process owner within the section of the CSC. So, if the organization was to establish the role of a process owner connected to GDPR, it makes sense to put this responsibility with a role who is located within the CSC. This might also be a good combination since the process owner is described as an employee with partly legal responsibility and also a say about what content should be put into the cloud based system.

In connection to the discussion about process owners, the use case in section 2.3.1 might be relevant. If process owners were to be established in the organization, these employees might make the easy deletion of customers' personal data possible. Since the process owners would know where the personal data is stored, at least within the processes where they are involved, it might make the deletion process a lot more efficient. It would also be easier to find information regarding who to contact if a customer was to make the request about deletion of data since there would be a name stated for the process owner. Hopefully, this can make sure that the customer's personal data is deleted in all systems where it is being handled.

Another insight that was stated by many interviewees was that personal data often today is stored in so called silos. A majority of participants state that it would be easier to track these types of data if it was stored with more structure within the organization. If personal data was to be stored in a way so that all relevant projects can reach it instead of each project storing the same data for themselves, this issue could be avoided. Since this is

something that also has been expressed by employees in the interview study, YIAS could once again take these suggestions into consideration. Since the employees' are the ones who handle the systems' firsthand it is important to listen to their suggestions and ideas.

According to many interviewees the importance of education on the topic also cannot be stressed enough. Education on the subject cover areas such as GDPR, personal data handling as well as how these types of data should be stored in a safe way. They were also considered great as introductions to the subject when first starting as a new employee at the company. Many employees expressed that these were good as reminders and also to make sure that each person receives the same information. Interviewees also requested education on what happens where there is a potential data breach. The understanding and knowledge regarding the process was in general quite mixed but a majority of participants requested education on the matter. So where there is room for improvement, employees are also motivated and interested in making a change. Further, the general perception is that the available courses on the matter are good and that employees would like to see more material that can be studied. Here, the virtual emergency drill that would be performed in case of a data breach could be helpful. Studying material is helpful but actually putting the knowledge to use in a practical scenario could be beneficial for employees and the company. This would allow the employees to put their knowledge to use as well as giving Vattenfall the opportunity to test their emergency response and processes.

Also, we did not see a correlation between data breach and the clarity of data ownership. However, it is clear that the awareness regarding data breach and what to do if it occurs has to increase amongst the employees. According to Figure 4, the majority of interviewees were marked as yellow or red. The goal is to make all these employees green but in order to achieve this, the awareness regarding the subject has to increase in the organization. It is very important to have clear routines and responsibilities if it was to happen in real time. Since the sequence of events can be very quick and much can be done early to decrease the impact of the breach, it is especially important to have a process in place. When a data breach happens it can then be contained and the damage can be minimized if you act quickly and this can be done if clear routines are in place. These routines are also good to practice beforehand so that all employees know how to act if a real situation was to happen.

The results from this study show that the standard could be suitable for YIAS. Vattenfall also has a previous international standard certification so deciding to add another version of the standard could be beneficial. Each responsibility role considered relevant can be filled with an employee within the department, all areas can be covered. It would also be suitable since the RA can help YIAS decide and part the responsibilities considering customers' personal data more clearly. Since the standard is also considered suitable for determining the ownership of data more clearly within an organization it can be stated that this could be applicable to YIAS.

So part of the recommendation for stating ownership more clearly within the organization is to use the international standard as a blueprint for the future. It would make the responsibilities regarding personal data clearer as well as make it easier to track usage of these types of data. If each employee involved in the RA has a clear picture of what responsibilities apply to them it could clear up a lot of confusion. Many of the improvements that can be done in order to make the handling of customers' personal data clearer also have been stated by employees themselves. These employees work daily with the digital systems and are therefore much aware of what can be done to improve them. Since these employees have great insight in the data handling within the cloud based systems it is important to take their opinions into consideration. Taking employees' suggestions and thoughts into account when presenting a recommendation is to be considered beneficial for YIAS since it emphasizes the importance of employees' wishes. This should lead to better solutions since they are based on employees' own perceptions of the data handling.

7. Discussion

Based on the findings on YIAS' existing architecture and employees' knowledge of data ownership, the following section presents a discussion of the results. The discussion focuses on the differences between the existing architecture and the one presented in the international standard. Improvements that can be made to improve security are also discussed.

7.1 How Close to the ISO/IEC 17789 is Vattenfall Customer IT Sweden?

The international standard provides guidelines for managing information security risks in organizations that are relevant to IT reference architectures. It can be used for establishing, implementing, maintaining and continuously improving a process. Generally, it is beneficial for a large organization to have a reference architecture that is aligned with the international standard because it demonstrates the company's commitment to managing information security risks effectively and applying best practice in this area.

This study of the YIAS department shows, that the existing organization's architecture and the standard are similar to each other. Based on the data collection and mapping of roles within the study's RA, it has been shown that there are clear connections in how the organization is divided. It can be concluded that YIAS can cover all responsibility roles of the standard. The fact that all roles are covered might be explained by the fact that several employees included in the study has previous knowledge of cloud reference architecture. Even if Vattenfall does not have a predetermined RA that they rely on in their organization, employees' knowledge of RA can contribute to the fact that all roles are covered even though it is not based on an RA. As there is no predetermined RA, there is a risk that the organization loses important responsibility roles and knowledge if they do not actively analyze and perform work based on an RA.

This study's role distribution for the YIAS presented in the results under section 6.1.1, has a role CSP: Peer Provider removed since the study's limitation around YIAS does not cover other Cloud Service Providers. Relied on the presented literature around the standard, the ownership of the data should belong to the CSC which means that the result would most likely remain unchanged if YIAS had Peer Cloud Service Providers. Based on the fact that it was possible to map the existing architecture within YIAS with RA, it demonstrates that YIAS is close to the international standard. This means that the company has implemented a system for managing information security risks that meets internationally recognized standards. For this reason, it is therefore of great relevance that Vattenfall obtains a certificate for the standard that demonstrates their knowledge of reference architecture. Since the RA can provide the organization with clearer responsibilities and understanding of who is responsible for data. It also gives

organizations greater confidence since a certificate within an international standard can be used in marketing. This can show their customers that the organization has the right skills and IT architecture in place. In turn, it increases the security of customers that the company stores the large amounts of data they collect from customers in a safe and secure way.

The certificate can provide several benefits, including improved credibility, increased trust, a competitive advantage, compliance with legal and regulatory requirements and continuous improvement. And a large organization like Vattenfall may choose to obtain certification for the standard for several reasons. But in general, it is beneficial to keep the delta between the organization and the standard small since it demonstrates the company's commitment to managing information security risks effectively and implementing best practices in this area. The certification also demonstrates that an improved credibility which can help the organization to improve the reliability with customers, partners, and other stakeholders. The increased trust that comes with the certification can help Vattenfall to increase trustworthiness in the ability to manage information security risks effectively. Which in lead can increase confidence in the organization's current products and services and feature products that may contain more customer data in a new context.

A certification can also provide the company with a competitive advantage since a certification demonstrates the organization's commitment to information security best practices. This might in turn can help the organization differentiate itself from competitors and win competitive advantages. Since the certification is an international standard it is also applicable to the whole organization and can hence be useful for all markets. This can help the organization demonstrate compliance with legal and regulatory requirements related to information security in the whole business. With the international standard, the organization has to establish and maintain an information security risk management process that is subject to continuous improvement. It can in return help to identify and address new and emerging information security risks in the market.

7.2 Security Improvements of Personal Data in the Cloud Environment

The finding that YIAS's IT reference architectures align with the international standard can help to ensure that information security risks are properly identified, assessed and managed as part of the architectural design and implementation process. This, in turn, can help prevent security breaches, data loss and other security incidents. All are aspects that can have a significant negative impact on an organization's reputation, operations and finances. From the interviews, it is stated that the process if a data breach occur is not clear enough for all employees. It is also stated that they ask for more information about the process as well as regulatory virtual emergency drills to increase their knowledge. This request comes from employees who handles Vattenfall's IT-systems. Hence it is

very important to listen to their needs since they are mentioning this information gap and it is fundamental information for all employees. Since the number of cyberattacks has increased recently it is even more critical to make sure all employees feel comfortable about what to do. The risk of sabotage against Vattenfall's IT and control systems is now considered to have increased. In February, Vattenfall's websites were subjected to denial of service attacks, and cyber criminality has increased and become more advanced. Therefore the process of actions has to be described more clearly.

Based on the international standard it has been possible to identify a data owner within YIAS. This study has analyzed employees' understanding of who the data owner is and the results show that it is something that needs to be improved since there is a lack of knowledge. In the analyses in section 5.5 it shows that the majority of the interviewees have not very clear or unclear knowledge regarding who the data owner is. Also, this study can conclude that based on the chosen RA, the data ownership within YIAS should belong to an employee within the section CSC. There is no science based result regarding if the ownership should belong to the whole group of people within CSC or just one specific person. However, the collected material from the interviews show there is a common suggestion that there is a need of process owners. Therefore this study does recommend YIAS to add process owners to the organization with their main responsibilities being placed within the CSC section. By adding process owners to YIAS it would give employees a better understanding of the ownership.

This in turn would solve the problem described in the user case described in 2.1.1 concerning deletion of data since it would make it clearer who to contact in this case. Today there are process owners for some processes but not for e.g. GDPR or data deletion. Since the organization is quite complex it is also hard to know if it would be enough with one person responsible for deleting customers personal data. The biggest flow when it comes to GDPR compliance is the data deletion and this is also mentioned as one of the biggest challenges by employees. One interviewee stated that "om en kund vill få all sin personliga data raderad vet jag hur jag ska göra för mina system men innebär det att datan raderas från andra delar av organisationen? Det kan jag inte svara på" [if a customer wants all their personal data removed, I know how to do this for my own systems but does that mean that the data is removed from other parts of the organization? I can not give a clear answer to this]. It is hard to say if process owners would solve this issue. A process owner can be responsible for the whole chain of events within a system but a process owner could never touch the data without speaking to the system owner first. However, a process owner could probably make the approach easier. People also mentioned that if you have an audit gap like that it can be solved if the ownership was stated more clearly. Since people have a good understanding about what type of data they are capturing regarding GDPR the next step is to automate how to delete certain types of information. Also the documentation about which GDPR data that is stored where could also be stated more clearly. In order to make that information transparent for all teams and what type of data that is stored and how to handle it.

Many interviewees also expressed a lack of understanding regarding the different types of personal data that Vattenfall handles. People usually think of a security breach as credit card information or types of PII but that is not always the case. In the energy industry, it is possible to access e.g. the temperature in a living space or information about when someone is home. If someone has access to all these types of data, it is very easy to get a lot of information about a person and their everyday life. This means that if the wrong person was to have access to a number of different data points it may cause a risk. This is rarely talked about but the fact is that with digitalization and the increase of the amount of information you can access. One can easily find multiple different types of information about another person. Today, we do not see the temperature in someone's home as a data breach but the fact that it reveals many other things about a person changes this. The aggregated data can pose a much greater threat than we realize. Having this information about a person means that e.g. politicians and high-profile individuals are increasingly vulnerable to blackmail. It is therefore important to have a great understanding of the data that Vattenfall is storing today. It is easy to get a visualization of the worst case scenario when all these different types of data re added together. Combining all this data can come with great consequences for the company but also the customers themselves.

Other security improvements in relation to customer's personal data people have identified or sought after is general security improvements. One improvement regards personal data and how to handle the audit gap that interviewees speak about, where they want a framework for how GDPR is managed. Another suggestion for improvement is to change the current security standard to private by default in all systems. This is to get control over access since it is easier to give user access than remove it. Privacy by default will secure the data from the beginning and keep it available for the right people. Encryption, as multiple interviewees mentioned can solve this and a process owner could be the one responsible for this as well. Also today, data is being replicated in different systems which is a future challenge to solve, since apart from that avoiding replicating data there is better to have a data marketplace where data can be shared between systems instead. Today the challenge lies with exporting data within systems since the security level the data has in one system might not apply in other environments. Hence, there has to be improvements so that the security authorization remains in both systems.

In everyday work life interviewees have also mentioned improvements regarding knowledge of sending personal information with email and how to handle CV's. Control over data disappears when it is sent data through email and that could be controlled better with use of SharePoint. Besides from that, another security improvement in relation to customers personal data is the identification and access management of customers portals. If cyber criminals were to target the customer portals, the identification and access management has to be improved and there are multiple controls that can be improved.

In conclusion, being close to the international standard can be beneficial for YIAS in order to effectively manage information security risks and demonstrate its commitment

to information security. Also, for a big organization like Vattenfall it can be beneficial when it comes to managing information security risks effectively and demonstrate its commitment to information security best practices. Generally, increased discussion about the responsibilities regarding handling customers personal data is a topic that should be made more relevant at a management level as well as development level. In summary, obtaining certification to the standard it can provide Vattenfall with several benefits, including improved credibility, increased trust, a competitive advantage, compliance with legal and regulatory requirements, and continuous improvement.

7.3 Recommendations and Implementation

After the discussion in sections 7.1 and 7.2 it is clear that some recommendations are easier to implement than others. They require different amount of resources which mean they also come with various risk. In order to implement the different recommendations stated, the potential risks have to be analyzed and evaluated. This compilation can be viewed in Table 2 a)-c).

Table 2. a) A compilation of recommendations for the First Line within the Three Line Model presented in section 2.3.1 which is responsible for executing the strategy and managing risks. This table will also present implementations and risk evaluation.

No.	Recommendation	Implementation	Risk
1.	Review and update the policies regarding personal data handling	Regularly update and review the current policies to ensure their relevance. Updates are recommended according to e. g. change in laws, business models or technological change.	▪ Needs to be done regularly to be effective ▪ Requires constant research ▪ Takes time and effort to change a policy within a company
2.	Virtual emergency drills	Performing virtual emergency drills successively for all parts of the organization. This is not relevant for only YIAS but for all employees since a data breach can happen anywhere. Stage a situation or create educational material that describes the process of a data breach and educate employees on how to act, in what order they should act and how to contain it.	▪ If the all employees were to practice this it will take time from their usual tasks ▪ Might be expensive if the whole company is affected
3.	Implementation of the international standard ISO/IEC 17789	Clear descriptions of responsibility roles and sections.	▪ Takes time to implement big changes into organizations ▪ Requires documentation and education since there is no set RA today

Table 2. b) A compilation of recommendations for the Second Line within the Three Line Model presented in section 2.3.1. The second line provides control, expertise, support, monitoring and challenge on risk-related matters. This table will also present implementations and risk evaluation.

No.	Recommendation	Implementation	Risk
4.	Implement a process owner who is responsible for GDPR processes	Name a process owner regarding GDPR legislations for digital systems. This person should preferably be from the CSC section of the standard.	▪ Needs a clear role description ▪ Uneven work load since a few employees have to be educated on the subject to take on the role ▪ Limited amount of employees who can take on this role since it should be in the CSC
5.	Implement a process owner who is responsible for deletion of data	Name a process owner for digital systems who is responsible for deletion of personal data. This employee makes sure that the deletion processes are being performed as expected and monitored.	▪ Needs a clear role description ▪ Uneven working load since a few employees have to be educated on the subject to take on the role
6.	Store personal data centrally so relevant employees can reach it	Make personal data storage centralized so each authorized employee can reach it instead of staff storing it for each project. Reduces the risk of duplications as well as it makes the sharing of data easier.	▪ Might need a new storage solution for the whole organization or IT department ▪ Expensive and resource consuming ▪ New routines that needs to be specified and documented ▪ Move the current data to a new solution ▪ Might affect the whole company
7.	Change the current security standard to private by default in all systems. Recheck access and automate deletion of access after a certain amount of time.	When deploying a system, the security standard should always be private. If this recommendation is implemented now, this will successively spread across all systems limiting access to relevant employees and stakeholders.	▪ Affects all digital systems to some extent ▪ Needs a pre-study as to what systems already deployed that needs this level of security

Table 2. c) A compilation of recommendations for the Third Line within the Three Line Model presented in section 2.3.1. The third line is made up of internal audit, which oversees and evaluates the first and second lines. This table will also present implementations and risk evaluation.

No.	Recommendation	Implementation	Risk
8.	Increased education and spreading of awareness	Involves e. g. better communication between employees and departments, regular audit of educational material, specify responsibilities etc.	▪ A lot of administration
9.	Invite relevant employees to e. g. stand ups in order to improve communication between departments and security managers. This will help increase the transparency.	Regularly, employees working with security should be invited to take part in e. g. discussions, workshops, stand ups or department meetings. This helps to spread awareness, discuss processes and remind staff of the responsibilities they have regarding personal data handling.	▪ No obvious risk
10.	Automate deletion of certain types of data	Prevents employees from having access longer than intended and limits the access to relevant staff. This could be done by process owners as well. Adding a process owner to this can help monitoring and making sure that it is being performed.	▪ The routines regarding this needs to be clearly documented
11.	Data encryption that protects personal data from unauthorized access	Identify the personal data that needs to be encrypted and based on this, choose a suitable encryption method. Also, encrypt data both in transit and at rest. If this is to be done, encryption keys also have to be well protected to avoid unauthorized access to data.	▪ The routines regarding this needs to be clearly documented
12.	Increased knowledge regarding different types of sensitive data	Education on how to handle information that at first glance might not seem harmful such as CV's, electricity consumption and files being sent by email	▪ No obvious risk

As can be viewed in the Tables 2a)-c) above, the recommendations are considered to differentiate in risk and belong to different lines of defense. As mentioned in section 3.2.1, the three line model is a part of Vattenfall's defense system. Each line of defense is made up of different responsibility roles who are incorporated in the defense. This also gives an idea of the priority each recommendation should have since the three line model secures the principle of segregation of duties and includes different roles for risk ownership, independent monitoring and control as well as assurance. As a complement to this, Figure 6 can also be viewed.

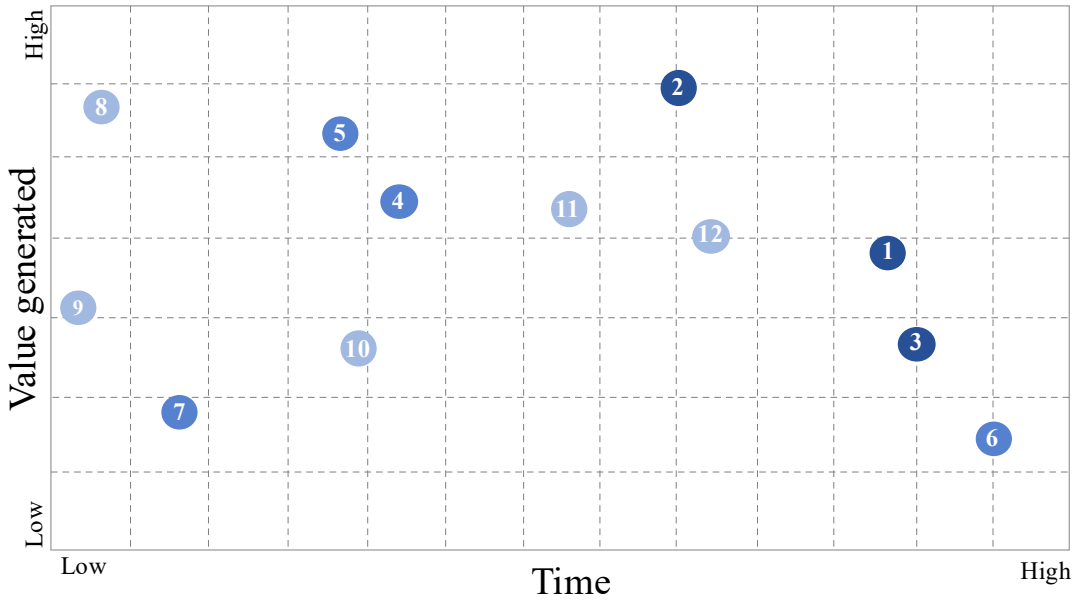

Figure 6. A scatter plot of the value generated of the recommendations mentioned in Tables 2 a-c). The color-coding corresponds to the Three Line Model described in the Tables above. Dark blue represents the First Line, medium blue represents the Second Line and light blue represents the Third Line.

Here, the generated worth for each recommendation has been approximated with the axes "time" and "value generated". So, Figure 6 shows how the time consumption for implementing each recommendation generates value for the YIAS department. Some recommendations are expected to be more time consuming than others however, the reward from the collected recommendations is expected to be high. From the reasoning in Tables 2 a)-c), the dots could be placed in the scatter plot and give an idea of the value created by the recommendations. The following sections implies how we have reasoned when placing the dots in Figure 6.

Number 6 is the recommendation expected to take longest time and it is a complex recommendation. Moving all personal data so it is stored centrally in the organization instead of in each system takes a lot of time and effort. Many systems will be affected and the whole organization might have to rethink how they get and store data. However,

if it was to be done it might save both time and resources. It could also decrease the risk of duplicating data or losing it since it would only be stored in one place.

The recommendation expected to create the most value is number 2, virtual emergency drills. A potential data breach would have great impact on the organization and could have a negative impact on customer's trust in Vattenfall. Since the consequences of this are considered to be great, the value created from spreading awareness regarding data breach is expected to be high. Since there is a lack of knowledge within the organization regarding routines and ways of working the virtual emergency drills are considered to create much value for Vattenfall. However, it might be quite a time consuming process depending on the approach. If educating material is to be created and then mandatory for all employees, staff has to take time from their working days to study the material. Say you would stage a data breach and employees were to practice the routines, the same applies regarding time consumption. Also, the whole organization has to take part in the education since a data breach is both not only limited to VIT but could also come from any department within the organization.

Looking at number 8 and 9, they are placed close to each other on the "time" axis but quite far apart on the "value created" axis. They are both considered to not be very time consuming but the generated value for the organization is a bit different. Starting with number 8, increased education and spreading of awareness regarding personal data protection. Most of the educating material regarding this is already created and mandatory to study for all employees however, it needs to be regularly updated and studied. Therefore it is considered to not be very time consuming since it is an ongoing process that does not have an end-date. Moving on to number 9 which is inviting relevant employees that work with data security related questions more often. Similarly to number 8, this is an ongoing process that needs to be done regularly to have an impact. The work load is limited to the invited employees who has to prepare and therefore the time consumption is low. However, the value created is considered to be quite high but not as high as for number 8. Since number 8 affects all employees the awareness regarding the topic is expected to spread and be more relevant to many. Inviting employees working with data security to e.g. meetings and stand-ups affects a few people at a time so the knowledge is not spread to as many employees.

7.4 Future Research

The cloud environment of YIAS will continue to develop which is an interesting area of study. Cloud services continuous development will affect how YIAS and Vattenfall as a company continues to build cloud environments and business requirements connected to them. Technology will continue to develop, hence many future solutions will be interesting to evaluate. The never ending development of new cyber threats will keep on affecting key role holders such as Vattenfall which makes data security continuously important. Investigating future versions of the cloud systems we have investigated now

would be interesting to see if any of the challenges we have identified in this study will be solved. It would have been interesting to see if we would have drawn other conclusions if other departments were studied or just larger sections of the company. So increasing the sample size for the interview study would be an interesting area of study as well.

Also, a new version of the ISO/IEC 17789 is under development as of May 2023. It is so far unclear as to when this is going to be available for the public but it does contain a fair share of updates and new concepts. It would have been very interesting to apply this new version of the standard on the YIAS department and compare to the finished one we have. Investigating potential differences or gaps between these would have been interesting. If this was to be done, we would have wanted to apply this version to YIAS as well in order to see if it would suit the department even better.

8. Conclusions

The following conclusions answer the research questions and complete the thesis. This section also states the lessons learned from working with the study as well as our final words.

8.1 Research Questions

How can a cloud environment architecture be organized in order to handle personal data?

According to this study, the gap between the current structure of the organization YIAS and the standard is narrow since all responsibility roles are covered. This means that YIAS has the chance to close the delta even more and by doing so, making the handling of customers' personal data even more clear.

In order to achieve a clearer data ownership and also make future development of the cloud environment easier, YIAS should determine a blueprint that employees can follow. Our suggestion for future work is to implement process owners as well as stating the responsibilities of each employee more clearly. Process owners will help to make the determination of who owns the personal data in each process easier since there will always be an employee stated as responsible for each process within the department. YIAS can also use the implemented RA to educate future employees on the subject since the responsibilities and processes will be stated more clearly within the department. When looking at Figure 4, one can see that the majority of the interviewees found the data ownership as not very clear. The same amount of participants found it clear as well as unclear. Therefore it can be concluded that most employees in this study does have somewhat of a good understanding of the data ownership within the organization. However, it is important to note that even though interviewees stated the data ownership as clear, all employees in this category declared different people as the owner. Interviewees hereby consider different employees and working roles as the owner of customers' personal data. If YIAS would focus the upcoming years on narrowing the delta even more between the current RA and the standard, this could benefit the department. As seen in the scatter plot in section 7.3 the suggested recommendations gives various amount of value for the company depending on time. These improvements will also help getting closer the delta and some of them generates value with only a small amount of time.

It can be concluded that there is a person considered responsible for each role in the standard however, there can be improvements. Mainly, since they are working agile the responsibility for each role has to be stated more clearly within the organization which will also make employees more comfortable in their given roles. Especially since some employees were considered relevant for an alternative role (see Table 1) a role description

with clear responsibilities is required. This would also help if an employee was to be replaced since the liabilities would be easy to pass on. There is already a great understanding amongst employees regarding cloud RA and this can be utilized going forward to implement a set RA.

It is important to note that the study has been done by investigating a small part of the Vattenfall organization. Therefore the results are not to be considered representative for the whole company and the conclusions drawn from this study might not be applicable to all parts of the organization. A main parameter that might have an effect on the result was the choice of employees for the interview study. Firstly, they all cooperate or work closely to the IT department at Vattenfall and therefore might have very similar experiences and knowledge. This does not necessarily have to be a bad thing but it might give a quite one sided picture of the situation. Secondly, we conducted 22 interviews with 19 different employees which can be considered a small sample size. The YIAS department is large so interviewing these employees might not give the whole picture since that would have required more interviews.

However, we received a positive picture of the current situation since the organization is most aware of the topic. All interviewees state that the subject is of most relevance and importance and they are motivated to make a change where needed. It is important to remember that eventhough a situation might be good, there are always improvements to be implemented and as seen in the scatter plot some of them are not time consuming. Therefore the organization have great opportunities when it comes to implementing these changes and working towards a set goal.

What actions can increase the security of personal data in the cloud environment within YIAS?

There are a few concluded factors that might improve the security of personal data in YIAS's cloud environment. To summarize, it all comes down to how the organization can make the people marked as red in Figure 4, yellow or green. In section 7.3 some recommended implementations was presented and all of them are in order to increase knowledge and security improvements. They are aligned with the three line model and presented in the scatter plot (Figure 6). This was done in order to see how much value the implementation of each recommendation gives as well as the time span of each.

Let's say YIAS adapts the standard over the upcoming few years, then the ownership of personal data should be placed with the CSC section. In order to determine who the main responsible working role should be, the department has to divide the employees according to the standard. Since each role has a description, dividing the department likewise would help with understanding who is most suitable. It would also show who has the most knowledge regarding the subject and therefore might be suitable for the responsibility position. The benefit is that employees placed in the CSC section generally have a quite good understanding regarding handling personal data. Therefore we believe the transition

into officially placing the ownership in the CSC section should be quite smooth. We also recommend that YIAS and Vattenfall encourages employees to study the educating material available on the subject since these were much appreciated by the interviewees. It would benefit the organization if employees were regularly reminded to study the educating material, this was also a wish from several interviewees.

The routines and processes are in place and employees generally have a good impression of these. However, everybody needs to be reminded of the responsibilities regarding handling these types of data as well as how to handle it. In order to spread awareness regarding the subject, one idea is to invite guest speakers to stand ups and department meetings which does not take much of time but generates valuable knowledge. E.g. security officers or employees who work daily with GDPR might help with keeping the subject top of mind. Another recommendation is that the organization updates the material with instructions of what to do if a potential data breach was to occur. If the processes and routines regarding the topic are stated clearly to all employees, Vattenfall and YIAS can improve this knowledge over the upcoming years and prepare all personnel on such an incident. These recommended improvements take more time to develop, but once they can be implemented, they provide great value. Doing this in combination with the suggested emergency drills on the situation can help the company increase the knowledge amongst employees over the coming years. Implementing the standard can, just like for the previous research question, provide the organization with a blueprint as to how the responsibilities regarding personal data can be divided. So hopefully, if a similar study was to be performed in a few years, the employees marked as red might be green.

Adding process owners to the data deletion process and GDPR related processes could also help with increasing the security and generates a high amount of value based on time. Since this would mean that a single person will have insight in the whole activity chain of a deletion process and make sure it is being carried out. This might also help with the traceability of information since the process owner will have full understanding of where the data is stored within a system. Also, if you would start to name a specific process owner for each potential deletion process now, it will gradually spread to all active systems. Increasing the awareness surrounding process owners can be achieved by e.g. inviting intended process owners to stand-ups or weekly meetings with groups working with specific systems. This way more employees will be aware of the working role and the process owner will gradually be introduced to the cloud systems where they are needed.

Whilst analyzing the information from the conducted interviews we realized that there were areas we wanted to know more about. It can be difficult to realize how important or valuable a statement from an interviewee is during an ongoing interview and this sometimes showed when looking at the collected data. Therefore we decided to contact multiple interviewees for further discussion regarding a few topics. This help to clear up

any confusion that had emerged from the interviews. However, contacting the interviewees again was time consuming.

8.2 Lessons Learned

When starting off this project we knew we wanted to learn more about RA and how it can be a beneficial tool for an organization. By performing this study we have gained knowledge of working with an international standard as well as how it might be implemented in a company. It has also shown us how theoretical frameworks can be applied on real life scenarios. Attempting to structure and divide responsibility within a department according to a set framework by us considered to be valuable knowledge.

This study has also given us great insight to one of the biggest companies in Sweden and how an organization like this can be structured. We have been given the opportunity to see an IT department's daily work and important data security actually is. Vattenfall handles big amounts of personal data every day and seeing how seriously employees and the organization as a whole work with this has been very interesting. It has really made us realize how important the topic is and that it cannot be stressed enough. An especially major insight we have come to is the fact how digital information that might seem harmless at first actually can be very dangerous in the hands of the wrong individual. Putting different pieces of information together can give a disclosing picture of a person. During our time at Vattenfall, we have also been given the chance to see how cyber-attacks are handled in real life. Cyber-attacks are increasing at the moment so seeing how different tools were put to use in such a crucial situation was very rewarding.

Lastly, this study has given us the opportunity to structure and perform a project over a longer period of time. Planning and estimating how long different parts of the study would take has been challenging. However, with good cooperation and communication it has been a smooth process.

8.3 Final Words

One interviewee stated that since the topics of personal data and information security are so abstract it is easy to lose track of what you are actually handling. This is something we have reflected upon as well whilst performing this study. When you are working with questions and information that is this complex, it is easy to lose track of what you are actually doing. So the feeling this interviewee is describing is something we recognize. Digging deeper into this topic and also to have been given the chance to experience how YIAS and Vattenfall work with these questions has been a rewarding experience. Also, employees have a general interest in the subject and are very well educated on these types of questions. So the recommendations presented in this study are potential improvements to an organization that is absolutely well functioning and well-informed about the topic.

Generally, this study has been much appreciated by employees. When we have reached out to employees for interviews or to collect other information, people have been very accommodating and helpful. Many employees stated in the interviews that our questions and study has been a great reminder as to why these topics are important especially during a time with various amounts of cyberattacks. It made employees reflect on the responsibilities regarding handling sensitive data as well as information security. The study has overall received great feedback and many employees have shown interest in our work and results which we have appreciated.

This study has provided a deeper understanding to how an RA can be constructed to improve personal data security as well as what actions can be done to achieve a secure environment. By providing recommendations as to what can be done, we hope that all employees of the department will be marked as green in the near future. We also hope that awareness regarding the importance of protecting customers' personal data can spread within the organization. Vattenfall employees are interested, well-educated and willing to learn about the topic. We hope that the organization can utilize these peoples' knowledge and the recommendations presented this study to achieve an even more conscious organization.

References

Abbas, N. & Andersson, J. (2015). *Architectural Reasoning Support for Product-Lines of Self-adaptive Software Systems - A Case Study*. [Online]. In: Weyns, D., Crnkovic, I. & Mirandola, R. (Red), Software Architecture - 9th European Conference (pp. 20-36). Dubrovnik/Cavtat, Croatia 7-11 September. Doi: 10.1007/978-3-319-23727-5.

Abrahamsson, P., Babar, M. A. & Kruchten, P. (2010). *Agility and Architecture: Can They Coexist?.* [Online]. IEEE Software, vol. 27, pp. 16-22. Doi: 10.1109/MS.2010.36.

Angelov, S., Trienekens, J. J. M. & Grefen, P. (2008). *Towards a Method for the Evaluation of Reference Architectures: Experiences from a Case*. [Online]. In: R. Marrison, D. Balasubramaniam & K. Falkner. Software Architecture - 2nd European Conference. Pisa, Italy 13-14 June. Doi: 10.1007/978-3-540-88030-1_17.

Bolander, E. & Frejas, A. (2015). *Diskursanalys*. In Bolander, E. & Thornberg, R. Handbok i kvalitativ analys. Stockholm: Liber, pp. 91-114.

Börjesson, M. & Palmblad, E. (2007). *Diskursanalys i praktiken.* 1st ed. Stockholm: Liber.

Cantone, G. & Alessandro, S. (2010). *Peaceful Coexistence: Agile Developer Perspectives on Software Architecture*. [Online]. IEEE Software, vol. 27, pp. 23-25. Doi: 10.1109/MS.2010.49.

Christensen, L., Engdahl, N., Grääs, C. & Haglund, L. (2010). *Marknadsundersökning: en handbok*. 3rd ed. Lund: Studentlitteratur AB.

Cyber risk countermeasures education (2021-12-08). *ISO/IE 17789 Cloud Computing Reference Architecture (CCRA).* Available at: ISO/IEC 17789 Cloud Computing Reference Architecture (CCRA) – Cyber Risk Countermeasures Education (CRCE) (cyberrisk-countermeasures.info) [2023-02-09].

Dagens Industri (2023-02-19). *Nya cyberattacker mot Sverige – "slår brett".* Available at: Anonymous Sudan riktar nya attacker mot Sverige (di.se) [2023-03-03].

Dalen, M. (2015). *Intervju som metod*. 2nd ed. Malmö: Gleerups Utbildning AB.

Forsgren, N., Humble, J. & Kim, G. (2018). *Accelerate - the Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations*. [E-book]. 1st ed. Portland: IT Revolution Press.

Fossey, E., Harvey, C., McDermott, F. & Davidson, L. (2002). *Understanding and Evaluating Qualitative Research*. [Online]. Australian & New Zealand Journal of Psychiatry, vol. 36(6), pp. 717-732. Doi: 10.1046/j.1440-1614.2002.01100.x.

Galster, M. & Angelov, S. (2015). *Understanding the Use of Reference Architectures in Agile Software Development Projects*. [Online]. In: Weyns, D., Crnkovic, I. & Mirandola, R, Software Architecture - 9th European Conference (pp. 268-276). Dubrovnink/Cavtat: Croatia 7-11 September. Doi: 10.1007/978-3-319-23727-5_22.

House of IT. (2021). *List of Acronyms*. [Online]. Available at: https://vattenfall.sharepoint.com/sites/HouseofIT/Lists/Acronyms/AllItems.aspx [2023-02-14].

International Organization for Standardization. (2014). *International Standard - ISO/IEC 17789*. Switzerland, Geneve: International Organization for Standardization.

Kochanek, M. (2002). *Data Center Delivery*. [Online]. Available at: Data Center Delivery (sharepoint.com) [2023-03-01].

Krüger, M. (n. d). *VDP – Vattenfall Digital Platform*. [Online]. Available at: VDP - Vattenfall Digital Platform (sharepoint.com) [2023-01-22].

Kvale, S., Brinkmann, S. & Torhell, S-E. (2014). *Den kvalitativa forskningsintervjun.* 3rd ed. Lund: Studentlitteratur AB.

Lindqvist, Z. (2002). *IT Governance*. [Online]. Available at: Data Center Delivery (sharepoint.com) [2023-03-01].

Lindvall, M., Basili, V., Boehm, B., Costa, P., Dangle, K., Shull, F., Tesoriero, R., Williams, L. & Zelkowitz, M. (2002). *Empirical Findings in Agile Methods*. [Online] In: Wells, D. & Williams, L., Extreme Programming and Agile Methods – XP/Agile Universe 2002 (pp. 197-2007). Chicago, Illinois: USA 4-7 August. Doi: 10.1007/3-540-45672-4_19.

Lynham, S. A. (2002). *The General Method of Theory-Building Research in Applied Disciplines*. [Online]. Advances in Developing Human Resources, vol. 4(3), pp. 219-376. Doi: 10.1177/1523422302043002.

Medvidovic, N. (2015). *Understanding the Use of Reference Architectures in Agile Software Development Projects*. [Online]. In: Wyns, D., Crnkovic, I. & Mirandola, R, Software Architecture - 9th European Conference (pp. 268-276). Dubrovnink/Cavtat Croatia 7-11 September. Doi: 10.1007/978-3-319-23727-5_22.

Medvidovic, N. (2015). *What Architecture Can Teach Us About When, Where, and Why Software Systems Decay*. [Online]. In: Wyns, D., Crnkovic, I. & Mirandola, R, Software Architecture - 9th European Conference (pp. 11). Dubrovnink/Cavtat: Croatia 7-11 September.

National Institute of Standards and Technology (NIST). (n. d.). [Online]. Available at: https://csrc.nist.gov/glossary/term/nsi [2023-03-03].

Nord, R. L. & Tomayko, J. E. (2006). *Software architecture-centric methods and agile development*. [Online]. IEE Software, vol. 23, pp. 47-53. Doi: 10.1109/MS.2006.54.

Noushandeh, Y. (2023-04-18). *Protecting privacy together*. [Online]. Available at: Protecting privacy together — Vattenfall Intranet [2023-02-06].

Pönisch, P. (2023). *Vattenfall Integration Platform*. [Online]. Available at: Vattenfall Integration Platform (sharepoint.com) [2023-03-01].

Svensson, L. (2022). *Data Protection Management*. [Online]. Available at: FI109.docx (sharepoint.com) [2023-02-20].

Svensson, L. (2023a). *Data subjects requests.* [Online]. Available at: Data subjects requests (sharepoint.com) [2023-02-16].

Svensson, L. (2023b). *International data transfers (Schrems II).* [Online]. Available at: International data transfers (Schrems II) (sharepoint.com) [2023-02-17].

Svensson, P. (2019). *Diskursanalys*. 1st ed. Lund: Studentlitteratur AB.

Talja, S. (1999). *Analyzing Qualitative Interview Data: The Discourse Analytic Method.* [Online]. Library & Information Science Research, vol. 21(4), pp. 459-477. Doi: 10.1016/S0740-8188(99)00024-9.

Vattenfall AB. (n. d.). *Vattenfall in brief*. [Online]. Available at: A brief summary of our key facts and figures - Vattenfall [2023-02-14].

Vattenfall AB. (2023). *Vattenfall's Digital Ten*. [PDF]. Available at: Vattenfall Digital Ten_ER_FK.indd [2023-03-03].

Vattenfall Eldistribution (n. d.). *Vi är Vattenfall Eldistribution*. [Online]. Available at: Om oss - Vattenfall Eldistribution [2023-02-16].

Vattenfall Customer IT. (2023). *Customer IT Organization.* [PowerPoint]. Available at: YIA-Updated-Feb-2023.pptx (sharepoint.com) [2023-01-20].

Vattenfall IT. (2020). *IT strategy*. [PDF]. Available at: VIT Strategy.pdf (sharepoint.com) [2023-02-14].

Vattenfall Press Office. (2022-04-22). *Focus in energy issues in Europe.* [Online]. Available at: Focus on energy issues in Europe - Vattenfall [2023-02-15].

Weyns, D., Mirandola, R . & Crnkovic, I. (2015). *Software Architecture – 9th European Conference*. [Online]. Dubrovnik/Cavtat, Croatia: 7-11 September. Doi: 10.1007/978-3-319-23727.5.

Wipf, J. (2023). *IT Glossary – DevOps*. [Online]. Available at: IT Glossary (sharepoint.com) [2023-02-27].

Zimmermann, S., Fitzner, D. & Kersten, M. (2018). *Tactical guide towards Cloud Computing Services.* [PDF]. Available at: Integration and Cloud Steering Board - Cloud_Tactical_Guideline.pdf - All Documents (sharepoint.com) [2023-02-20].

Appendix A. Interviews

Table 3. An anonymized table of interviews conducted in the study.

No.	Role	Date for interview
1	Manager	16 January-8 May, 2023
2	Manager	26 January, 2023
3	Manager	30 January, 2023
4	Manager	30 January, 2023
5	Manager	1 February, 2023
6	System architect	9 February, 2023
7	System architect	13 February, 2023
8	Developer	7 March, 2023
9	System architect	9 March, 2023
10	System architect	10 March, 2023
11	Manager	13 March, 2023
12	Developer	13 March, 2023
13	Security and risk	14 March, 2023
14	Manager	14 March, 2023
15	Solution architect	15 March, 2023
16	Developer	15 March, 2023
17	Manager	17 March, 2023
18	Developer	20 March, 2023
19	Developer	20 March, 2023
20	Manager	21 March, 2023
21	Manager	22 March, 2023
22	Security and risk	4 April, 2023

Appendix B. Interview Guide

Interview Guide

- Present us and the project.
    - Master's of science in sociotechnical systems engineering (STS) at Uppsala university with a master's within IT.
    - This project started in January and will continue until the end of May. The purpose of this master thesis is to investigate the Swedish part of the cloud environment at Vattenfall Customer IT Sweden (YIAS) focusing on determining the ownership of personal data. By creating a recommendation for how the cloud architecture should be built in order to keep the ownership of the personal data clear, YIAS can **improve** its cloud solutions and business goals.
    - This thesis is going to be public when published and Vattenfall will read through the report to make sure we are not mentioning any security information.

- Can we record this interview?
- One of us will take notes during the interview.

Background questions

- Briefly describe your role and your current work tasks.
    - For how long have you had your current role?
- Have you had any previous roles within the Vattenfall organization and how long have you been working for the company?

Cloud Enterprise Architecture in a Reference Architecture Context

Personal data

Personal data - are data that can be traced directly or indirectly to an individual person, such as name, address and place. A personal data breach is a breach of the safekeeping of personal data such as its loss, theft or unlawful processing.

- Do you have any ongoing projects handling customers' personal data?
- What is your perception when it comes to Vattenfall Customer IT working with customers' personal data in the cloud?
- Do you as an employee reflect on the responsibility regarding handling customers' personal data when working in the cloud?
    - If **yes**, evaluate.
    - If **no**, why not?
- Within your work, what are the different components that are being used for handling customers' personal data?
    - How do these components interact with each other?
    - Is this a reasonable way of storing sensitive information according to you?

Current architecture

- Do you know what responsibilities you have as an employee regarding customers' personal data?

    - Do you find the current responsibilities regarding customers' personal data clear?
- Do you know who the owner of the customers' personal data is?

Future architecture

- Have you thought of any improvements regarding current enterprise architecture when it comes to handling customers' personal data? Any suggestions?
- In what way do you think the ownership of customers' personal data could be stated more clearly within Vattenfall Customer IT?
- Is the responsibilities regarding handling customers' personal data a topic that is being discussed?

In an ISO/IEC 17889 Context

General questions

- Do you have specific regulations that you follow when designing the cloud in relation to customers' personal data?
- In your working role, how do you maintain keeping customers' personal data safe in the cloud environment?
- Do you normally test personal data requirements after implementing new changes within the environment?
- Would you describe your role and work tasks as more **organizational** or **technical**? Could you explain how?
    - If **yes** to **organizational**, ask questions about blue and orange
    - If **yes** to **technical**, continue with questions under green
- The regulations you follow regarding customers' personal data, do they usually come from business (Such as distribution or heat) or from IT?
    - If **yes**, could you explain what this relation looks like?
- Do you have a business relation to any of the Vattenfall business departments?
    - If **yes**, could you describe your business relation with the relevant business departments of Vattenfall?

      Cloud Service Customer (CSC) - has a business relationship with a cloud service provider for the purpose of using cloud services. A cloud service customer can also have a business relationship with a cloud service partner for a variety of purposes.
        - Do you think of yourself as the owner of the customers' personal data? Or do you consider the business side as the owner? Someone else?
    - If **no**, could you explain why?

- Do you handle the product which is presented to the end user?
    - If **yes**, can you give an example of such a product and what functions it has?

  Cloud Service Provider (CSP) – makes cloud services available to cloud service customers. This role (and all of its sub-roles) focuses on the cloud computing activities necessary to provide a cloud service and the cloud computing activities necessary to ensure its delivery to the cloud service customer, as well as cloud service maintenance. The cloud service provider is responsible for dealing with the business relationship with cloud service customers.

- Which work area do you find most suitable for you and your daily tasks:
    - Managing
    - Maintenance and service of cloud environment
    - Deployment of/in cloud services
    - Security and risk evaluation in the cloud environment
- Can you describe customers' personal data in relation to this specific work area?
- If **no**, could you explain why?

- Do you work with deployment or audit/provision of cloud services?
    - If **yes**,

Cloud Service Partner (CSN) – is a party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both. A cloud service partner's cloud computing activities vary depending on the type of partner and their relationship with the cloud service provider and the cloud service customer.

- Can you explain how?
- Can you describe customers' personal data in relation to your specific work area?

    - If **no**, could you explain why?

Security

- Are there any security improvements in relation to customers' personal data you have identified or sought after? Generally or system specific.
- Are there any organizational changes you would like to see in relation to the handling of customers' personal data?
- Are there times when you discovered a security vulnerability in the cloud-based system which stores personal data?
- What do you and the organization do when there is a data breach?

Other

- Is there anything you would like to add?
- Can we contact you for further clarifications?
- Any questions to us?

Appendix C. Intervjuguide

Intervjuguide

- Presentera oss och projektet.
    - Civilingenjör i system i teknik och samhälle (STS) vid Uppsala universitet med inriktning på IT.
    - Detta projekt började i Januari och kommer fortgå till slutet av Maj. Syftet med projektet är att undersöka en del av molnstrukturen på Vattenfall Customer IT Sverige. Arbetet kommer fokusera på att bestämma ägandet av personlig data. Vi kommer att försöka skapa en rekommendation för hur den moln arkitekturen ska se ut för att göra ägandet av personlig data tydlig och säkert. Det här är ett behov som finns att undersöka enligt avdelningen, därför intervjuar vi personer som arbetar i den här miljön.
- Vi kommer skriva två rapporter där den ena kommer bli publikt och då kommer Vattenfall att läsa igenom arbetet för att försäkra att det inte finns någon konfidentiell information.
- Kan vi spela in denna intervju?
- En av oss kommer leda intervjun medan den andra kommer anteckna.

Bakgrundsfrågor

- Beskriv din roll och dina nuvarande arbetsuppgifter översiktligt.
    - Hur länge har du haft din nuvarande roll?
- Har du haft tidigare arbetsroller inom Vattenfall och hur länge har du arbetat på företaget?

Cloud Enterprise Architecture i ett Referens Arkitektur Kontext

Personlig data

Personlig data – data som kan spåras direkt eller indirekt tillbaks till en individuell person såsom namn, adress och plats. Ett läckage av personlig data äventyrar möjligheten att hålla personlig data säker genom att den går förlorad, stöld eller olaglig processering.

- Har du några pågående projekt som hanterar kunders personliga data?
- Vad är din uppfattning gällande YIAS arbete med kunders personliga data i molnet?
- Reflekterar du som anställd över ansvaret som kommer med att hantera kunders personliga data när du arbetar i molnet?
    - Om **ja**, utveckla.
    - Om **nej**, varför inte?
- I ditt arbete, vilka olika komponenter finns för att hantera kunders personliga data?
    - Hur interagerar dessa komponenter med varandra?
    - Är detta ett rimligt sätt att hantera känslig information på enligt dig?

Nuvarande arkitektur

- Vet du vilka ansvar du har vid hanteringen av kunders personliga data som anställd?

    - Uppfattar du det nuvarande ansvaren gällande kunders personliga data som tydligt?
- Vet du vem ägaren av personlig data är?

Framtida arkitektur

- Har du tänkt på några förbättringar gällande nuvarande organisationsstruktur när det kommer till hanteringen av personlig data? Några förslag?
- På vilket sätt anser du att ägandet av personlig data skulle kunna bli mer tydlig inom YIAS?
- Är ansvaren gällande hanteringen av kunders personliga data ett ämne som diskuteras?

I en ISO/IEC 17889 Kontext

Generella frågor

- Har du några specifika regelverk som du följer när du designar molnmiljön kopplade till kunders personliga data?
- I din arbetsroll, hur uppehåller du säkerheten kring kunders personliga data i molnmiljön?
- Testar du vanligen kraven kopplade till kunders personliga data efter att nya förändringar har publicerats i miljön?
- Skulle du beskriva din roll och arbetsuppgifter som mer administrativt eller tekniskt? Kan du förklara hur?
    - Om **ja** till **administrativt**, fråga frågor om blått och orange.
    - Om **ja** till **tekniskt**, fråga frågor under grönt.
- De regelverk du följer som gäller kunders personliga data, kommer de vanligtvis från IT eller business sidan (distribution, heat)
    - Om **ja**, kan du beskriva hur den relationer ser ut?
- Har du ett samarbete med någon av Vattenfalls avdelningar som arbetar med business (distribution, heat)?
    - Om **ja**, kan du beskriva ditt samarbete med dessa avdelningar?
      Cloud Service Customer (CSC) - has a business relationship with a cloud service provider for the purpose of using cloud services. A cloud service customer can also have a business relationship with a cloud service partner for a variety of purposes.
        - Anser du dig själv vara ägaren av kunders personliga data? Eller skulle du säga att business sidan är ägaren? Eller någon annan?
- Om **nej**, kan du förklara varför?

- Hanterar du produkterna som blir tillgängliga för slutanvändaren (kunden)?
    - Om **ja**, kan du ge ett exempel?
      Cloud Service Provider (CSP) – makes cloud services available to cloud service customers. This role (and all of its sub-roles) focuses on the cloud computing activities necessary to provide a cloud service and the cloud computing activities necessary to ensure its delivery to the cloud service customer, as well as cloud service maintenance. The cloud service provider is responsible for dealing with the business relationship with cloud service customers.
- Vilket arbetsområde anser du passar bäst in på dig?
    - Hantering av data

    - Underhåll och service av molntjänster
    - Utbyggnad och uppgradering av molntjänster
    - Säkerhet och risk evaluering inom molntjänster
- Kan du beskriva kunders personliga data i relation till det av dina specifika affärsområden?
- Om **nej**, kan du förklara varför?

- Arbetar du med utbyggnad eller provision av molntjänster?
    - Om **ja**,
        - Cloud Service Partner (CSN) – is a party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both. A cloud service partner's cloud computing activities vary depending on the type of partner and their relationship with the cloud service provider and the cloud service customer.
        - Kan du förklara hur?
        - Kan du beskriva kunders personliga data i relation till ditt specifika affärsområde?
    - Om nej, kan du förklara hur?

Säkerhet

- Finns det några förbättringar gällande säkerhet i relation till kunders personliga data som du har identifierat eller önskar fanns? Generellt inom organisationen eller mer systemspecifikt.
- Finns det några organisatoriska förändringar du skulle vilja se i relation till hanteringen av kunders personliga data?
- Har det uppstått situationer när du har identifierat sårbarhet kopplat till hanteringen av kunders personliga data?
- Vad gör du och organisationen när det sker ett dataintrång?

Annat

- Finns det någonting mer som du vill lägga till?
- Kan vi kontakta dig för vidare frågor och funderingar?
- Har du några frågor till oss?