Master

Investigating Cloud Access Security Broker In A Healthcare Service

Creating A Cloud Access Security Broker (CASB) Discussion Framework For Evaluating Security in Cloud Healthcare Services

THEODOR FOSSUM & VALDEMAR ANDERSEN

SUPERVISOR

Paolo Spagnoletti

University of Agder, 2021
Faculty of Engineering and Science
Department of Engineering and Sciences

Obligatorisk gruppeerklæring

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

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

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).

Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

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

Acknowledgements

We wish to thank our supervisor Paolo Spagnoletti, without whom the project would never have been completed. He provided very insightful guiding and immensely important feedback.

We wish to thank the supervisors from Sykehuspartner for great support and discussions in the creation of this thesis. Without their help, this work would not have been possible. The super-team from Sykehuspartner consisted mainly of: Christian Jacobsen, Øystein Balstad, Steinar Watne og Sturla Berg.

Furthermore, we would like to thank Peter Crook and Kjetil Nordlund from Microsoft Norway for taking time to explain important aspects around CASB.

In addition, we wish to thank Sondre Glimsdal for invaluable feedback.

Last but not least, we wish to thank our friends and families for immense support through the roller coaster of emotions that this thesis has brought upon us. Thank you so much.

Abstract

Covid-19 accentuated the importance of accessible services, causing a major increase in the adoption of cloud services for enterprises. Cloud computing is a new paradigm that promises significant benefits for organizations in healthcare services. However, cloud computing also transforms enterprise architectures and introduces new problems of information security. Decision-makers in a large healthcare service provider need to justify decisions on cloud adoption, but such a task is convoluted given the different views on cloud computing and the potential impact of cyberthreats on critical infrastructures. As a consequence, cloud security controls need to be selected and implemented to complement cloud services. Our research focuses on the decision-making process for selecting a Cloud Access Security Broker (CASB) in a large public healthcare ICT provider in Norway. This thesis applies Action Design Research (ADR) to design a decision support tool for cloud security control selection in healthcare organizations. The result is a framework for evaluating cloud security controls that facilitates the decision-making process by considering multiple aspects of enterprise security architectures. Participants in the decision-making process can achieve a common understanding of cloud security control and a tailored assessment of how the cloud will impact information security in the organization. We present the design process and apply the framework to the CASB selection problem. As a practical implication, our findings suggest that selecting a cloud security control in a healthcare service provider is an ill-structured or "wicked" problem that requires a unique problem-solving approach.

Contents

List of Figures

List of Tables

Glossary

AAC Adaptive Access Control. xvii

AD Active Directory. xvii

ADR Action Design Research. xvii

ADT Intrusion Detection System. xvii

API Application Programming Interface. xvii

BIE Building, Intervention and Evaluation. xvii

BYOD Bring Your Own Device. xvii

CASB Cloud Access Security Broker. xvii

CEO Chief Executive Officer. xvii

CERT Computer Emergency Response Team. xvii

CIA Confidentiality, Integrity, Availability. xvii

CISO Chief Information Security Officer. xvii

CSA Cloud Security Alliance. xvii

CSC Cloud Service Customer. xvii

CSP Cloud Service Provider. xvii

DLP Data Loss Prevention. xvii

DOI Diffusion of Innovation. xvii

DoS Denial-of-Service. xvii

EHR Electronic Health Records. xvii

EPR Electronic Patient Record. xvii

ER Emergency Room. xvii

EST Intrusion Prevention System. xvii

EST Virtual Private Network. xvii

GP General Practitioner. xvii

HIE Healthcare Infrmation Exchange. xvii

HTA Health Technology Assessment. xvii

IAM Identity and Access Management. xvii

ICT Information and Communications Technology. xvii

IT Information Technology. xvii

KPI Key Performance Indicator. xvii

MCAS Microsoft Cloud App Security. xvii

NGFW Next/Generation Firewall. xvii

OWASP The Open Web Application Security Project. xvii

PBMA Program Budgeting and Marginal Analysis. xvii

PSRA Priority Setting and Resource Allocation. xvii

QoS Quality-of-Service. xvii

ROI Return of Investment. xvii

SECaaS Security-as-a-Service. xvii

SLA Service Level Agreement. xvii

SMB Small and Medium Businesses. xvii

SWG Secure Web Gateway. xvii

TOE Technology Organization Environment. xvii

UEBA User and Entity Behaviour Analytics. xvii

UTM Unified Threat Management. xvii

WAF Web Application Firewall. xvii

Chapter 1

Introduction

1.1 Motivation

This thesis will use an Action Design Research (ADR) method to create a framework supporting decision-makers in a large healthcare organization. The reason is that Sykehuspartner, a large healthcare ICT service provider in Norway, wishes for input in the decision-making process related to the purchase and adoption of a cloud security technology. The technology in question is a Cloud Access Security Broker (CASB), which is advertised as one of the most promising cloud security technologies at the time of writing. However, Sykehuspartner, as a large healthcare organization looking to adopt cloud security solutions, has not yet adopted CASB into its cloud environment. So is the problem originating in the decision-making process of Sykehuspartner, or is the problem originating in the CASB technology? Is a CASB worth buying? This thesis seeks to answer these questions. We create an overview of the CASB technology to understand the different functionalities it can provide.

When a new technology is praised for fixing many fundamental problems in cloud security, it is natural for a leading security official in a large healthcare organization to evaluate if the technology can benefit the healthcare organization. So what must be in place before a new technology is approved for adoption? Additionally, how can one ensure that the best possible choice has been made?

Findings in this project will be relevant to test the maturity and applicability of CASB by placing it in a setting of a large healthcare organization. CASB providers and security professionals evaluating the need for a CASB will gain more insight from this thesis. The findings will also be relevant for large healthcare organizations as the resulting framework is intended to improve the decision-making process in such organizations in general. Therefore, this thesis will provide insight into the decision-making that is going on in a large healthcare service provider.

1.1.1 Gap in Literature

Documentation on CASB mainly provided by the vendors, and as such, can be viewed as advertisements. Research explains the possible benefits that a CASB can provide and research that details possible deployment modes of the technology. However, little research focuses on the applicability of a CASB in a real-life scenario, verifying that CASB is an up-and-coming technology that every large organization soon will use. Therefore, it is insufficient research to back up the claim that a CASB provides value for large organizations, especially a large healthcare organization. Therefore, organizations and businesses utilizing CASB can not be sure that a CASB provides more value than other competing technologies or if a CASB provides any value at all.

There is a need for studies that focuses on closing the gap between research and practical applications, and a method that focuses on the combination of theory with practice is Action Design Research (ADR) (Sein et al. 2011).

1.2 Background

1.2.1 The Transition of Healthcare Services Cloud

The healthcare organizational structure is distributed by nature, as different locations provide different levels of healthcare services. For example, while hospitals are needed to treat critically ill patients, several other instances are needed, from everything to follow up on patients in rehabilitation to emergency wards and individual general practitioners (GP's). This means that data is aggregated at several different geographical locations and might be needed at a completely different location. An example being a GP diagnosing a broken limb, sending the patient to a hospital for an X-ray scan and possible surgery. For the most efficient treatment, the hospital must get all the aggregated data from the GP, but transferring patient healthcare data is not straightforward. The transfer system must be robust and secure to ensure no leaks or loss of patient data ensues. There is also an inherent problem of data ownership, as the healthcare service provider itself rarely develops the technology that is best suited for healthcare information exchange (HIE). Therefore, the HIE must pass through technology owned by organizations or businesses that might have nothing to do with healthcare service. The step that transfers data from one healthcare service provider to another then becomes vital both because when data leaves the premises of a healthcare service provider, it loses control over the data while still being responsible for the data. The process of HIE between healthcare service providers can also be essential to ensure efficient treatment, especially in the scenario of an ambulance being an entity that sends healthcare patient data to the emergency room (ER). There are solutions for this already, although cloud services will enhance the capability even further. In the notion of HIE, there already exists solutions on the premises of different healthcare service providers, so the eventual process of utilizing the cloud will be to migrate the existing services into cloud infrastructure. Both cloud migration and cloud adoption are a part of the transition from on-premises computing to cloud computing. Cloud migration is the part of moving existing services and data from on-premises hardware to cloud-based infrastructure. Cloud adoption is the notion of adopting cloud services from third-party actors.

1.2.2 Why Cloud

When Covid-19 hit the world with increasing strength in the winter and spring of 2020, it soon forced people into their homes. The enforcement stemmed from lockdowns to prevent further infections. These lockdown measures forced enterprises across the world to either adapt or face severe economic consequences. Seemingly every business that had the opportunity moved to a work-from-home model, forcing businesses to facilitate remote working, leading to a significant increase in digitization of businesses. This shift accelerated cloud adoption plans, meaning that cloud computing has become even more critical for enterprises as the value of remote working was highlighted during the lockdown.

Cloud computing is a paradigm of computing that enables easier sharing of data and computing resources and is therefore very relevant to healthcare service providers as electronic health records (EHR) are growing in popularity. Cloud computing will allow for easier sharing of information, such as EHR, between employees and the healthcare service organizations themselves.

1.2.3 Threats against Cloud

Threats

Hong et al. 2019 states that: "The cloud overcomes many limitations of the traditional network, such as scalability and adaptability, by simplifying the resource management and control, as well as reducing the cost of implementations. However, the new infrastructure brings various threats, both existing and new, ultimately increasing the complexity of security management." In their paper, they discuss different attack scenarios on cloud components in a CSP.

Attacks can stem from many sources, but the most critical attack vectors are highlighted by Coppolino et al. 2017: External users, internal users, and the CSP itself. Open issues for cloud computing are found in the Coppolino et al. 2017 study: Shared technologies vulnerabilities, data breach, account or service traffic hijacking, Denial-of-Service (DoS), and malicious insiders.

The advantages of cloud computing can quickly become threats if not implemented or controlled correctly. For example, availability can be a major threat due to a cloud service utilizing the Internet. In other words, the cloud enables the connection of unsanctioned devices, and unsanctioned devices can be both an advantage and a threat, with the perception of which unsanctioned category devices fall under being interpreted differently by every person in the organization. It is, therefore, a benefit to make sense of the threats and new technologies to create a common understanding between stakeholders before a decision on adoption is made.

Answering Threats in Cloud

There are many different options to mitigate risk in cloud solutions. A logical step when investigating security in cloud computing is to evaluate a solution that resides not in the existing security environment that secures on-prem services, neither in the CSP environment, but in between. In other words, a cloud security technology that functions as an intermediary for the cloud customer and cloud provider, only focusing on the security of the communication and storage of data. Brokering is a form of intermediary technology, and a broker that focuses on security is a Cloud Access Security Broker (CASB).

1.2.4 Decision Making on Cloud Security Controls

The Internet continues to be a revolutionary invention that changes people's behavior almost overnight. A company or private person who wants to host a service on the Internet will cross into Cloud Computing at some point. They might find that the service can be hosted directly in a tailor-made cloud environment, or the service can be further enhanced by applications that utilize the cloud. For a company that wants to use the Internet, there is a high probability of interacting with cloud computing in some shape or form. However, the field of cloud computing is moving quickly, and decisions have to be made at the same tempo.

For a private person hosting a cloud service, fewer decisions have severe consequences than for a Chief Information Security Officer (CISO) in a large organization. A CISO or other leading security officials have areas of responsibility that are imperative for an organization's existence. Decisions made by a CISO are very significant as they, in the scenario of a healthcare service provider, impact critical infrastructure. However, a CISO is not the top executive owning the responsibility of an organization. Meaning that a top executive, a Chief Executive Officer (CEO), has a powerful incentive to observe and influence the decisions a CISO makes as the decisions impact the organization, and by that, the CEO. The main area of responsibility of a CISO is to manage the information security risk for the organization. The connection with the main risk owners, which is the top-level management in the form of a board or CEO, means that every decision must be thoroughly evaluated. The aspect of time is also essential to consider, as the decisions will, in most cases, have strict deadlines that accompany them. Either set by an executive board or external factors such as, but not limited to, the release of a new computer virus.

For a CISO or other security decision-makers to make a good decision, it is vital to have good support during the decision process. A good decision will be a decision that increases the security or increases the quality of the service that can be provided. It might therefore seem like a straightforward task to decide when the aim is to improve. However, a good decision is much more complicated as the outcome of a decision is not clear beforehand. For instance, in the adoption of new security technology, it can be debated how well the new technology will enhance the organization's security. On one side, it can be argued that the new technology will fit into the existing infrastructure and improve security; on the other side, it can be argued that it will conflict with the environment that it is deployed in creating new vulnerabilities. Such a question is proportionately hard to answer based on how large the environment is and is a considerable challenge for large healthcare providers. Every new decision on technology adoption must, in that case, be justified as improving the healthcare service enough to make it viable for purchase.

In the case of a large healthcare organization, the justification of new technology will be influenced by opinions from many stakeholders that might represent very different areas of interest. Technology must comply with legal regulations, security, economic interests, and most importantly, patient welfare together with the technical considerations of the legacy systems that already exist in the infrastructure. It is also crucial that vulnerabilities introduced by new technology do not exceed the organization's risk appetite. Risk appetite is a term used to represent how much risk an organization is willing to accept, as there is no such thing as zero risks. We, therefore, suggest that a common understanding of what the technology is and what the technology can accomplish will be beneficial for decision-makers in a large healthcare service organization. Therefore, this master project creates a Decision Support Framework to help persons in large healthcare service organizations make the best decision for the organization.

1.3 Research Goal

Our work responds to the apparent gap in the literature of a practically oriented study and design approach to help organizations reach a justifiable decision to adopt new cloud security technology. With the case being Sykehuspartner's wish to justify the adoption of a CASB. The goal for this project is, therefore, to:

- Identify how a common understanding can benefit decision making on the adoption of new cloud security technology for a public healthcare service provider

To reach the Research Goal, we ask the following Research Question:

- How can we create a common understanding for decision-makers, in a public healthcare service provider, in the process of adopting a new cloud security technology?

1.4 Scope

- The report will focus on cloud applications, with an emphasis on cloud security applications.
- Organizations that are of interest in this report are Healthcare Service Providers.
- The technology focus is limited to the adoption of cloud security technology. The purpose is not to analyze and investigate the technologies in a deeper aspect than is necessary for the explanation part of the framework.

1.5 Report Outline

- ***Chapter 1* - Introduction:** introduces the reader to the problem and the motivation for the project.
- ***Chapter 2* - Literature Review:** gives state of the art for both the field of cloud computing in healthcare and how an organization decides when to buy a new technology to meet business needs.
- ***Chapter 3* - Methodology:** gives an explanation of the method used to answer the Research Question; Action Design Research. The aim is to explain why ADR is useful for the project, what ADR consists of, and whom the team consists of.
- ***Chapter 4* - Problem Formulation:** defines the problem in the ADR process that the artifact is answering, and then the larger class of problems the newly defined problem belongs to.
- ***Chapter 5* - Building, Intervention, and Evaluation:** detail the ADR process of Building, Intervention, and Learning which explains how the artifact was created.
- ***Chapter 6* - Reflection and Learning:** highlights the learning that has emerged from reflection on the different stages of the ADR process.
- ***Chapter 7* - Formalization of Learning:** evaluates the viability of our findings and the usability of the Decision Support Framework.
- ***Chapter 8* - Conclusions:** gives a closing statement on the Decision Support Framework and the contributions from the project work.

Chapter 2

Literature Review

In this chapter, the relevant literature for the research is highlighted. Figure 2.1 explains how the different topics of healthcare, CASB, and decision making tie together. The articles discussed in this chapter will enlighten the theory around artifact creation and provide insight into the relevancy of the project work.

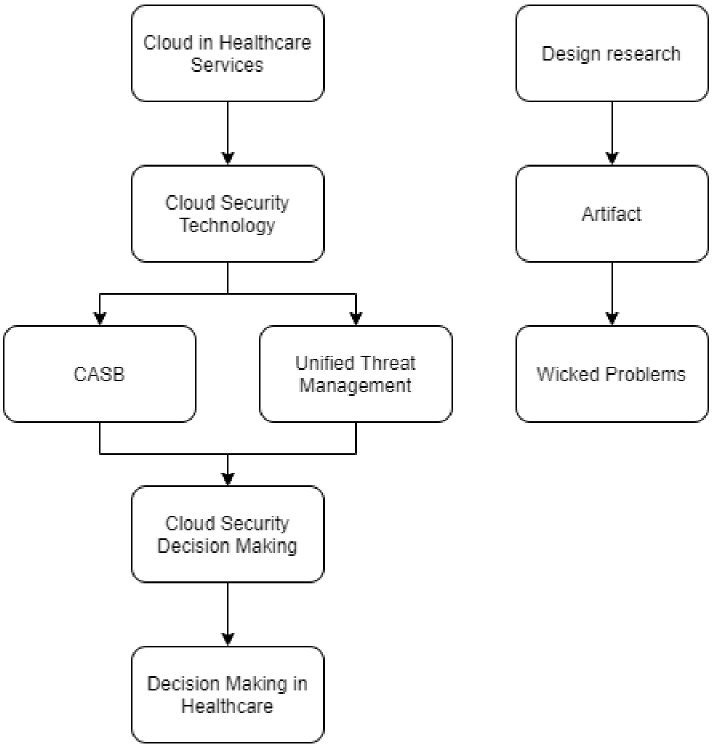

Cloud in Healthcare Services
Cloud Security Technology
CASB
Unified Threat Management
Cloud Security Decision Making
Decision Making in Healthcare
Design research
Artifact
Wicked Problems

Figure 2.1: *Flow of topics in Literature Review*

2.1 Cloud In Healthcare

Cloud computing for healthcare is seen as an important step forward for healthcare service providers, thus its implementation and adoption are discussed all around the world [Ramírez et al. 2016, Al Mudawi, Beloff, and White 2019, Peng, Dey, and Lahiri 2014, Ouardi, Sekkaki, and Mammass 2017].

Healthcare service providers are trying to deliver a more affordable and efficient healthcare system, with the intention of easily shared patient data between patients and other healthcare service providers according to Chang, Chou, and Ramakrishnan 2009. In order to finalize this sharing securely, Chang, Chou, and Ramakrishnan 2009 implies that it is essential to develop secure IT systems that can enhance this sharing between organizations. In that regard, the authors claim that cloud computing is a suitable IT solution for this kind of task since the emergence of cloud computing is in the wind right now.

Cloud computing replaces traditional healthcare service methodologies in the form of smart healthcare clouds, according to Chauhan and Kumar 2013. SaaS applications are suitable for a doctor and patient environment that is quickly changing. Chauhan and Kumar 2013 finds benefits and challenges with this change in healthcare service methodology. Benefits of health clouds include low-cost computing service, improved performance, low cost of IT infrastructure, fewer maintenance issues, universal access, and effective collaboration. Challenges of health clouds include proper bandwidth, user acceptance, security, and big data mining. Fabian, Ermakova, and Junghanns 2015 states that the age of cloud computing matches the needs of collaborating healthcare employees, despite the many security and privacy challenges that prohibit widespread cloud adoption.

Rizk et al. 2020 also highlights the increasing interest in cloud computing in healthcare while further explaining that it is due to the affordable cost and enormous data storage capabilities. At the same time, there is no standard practice to format the cloud computing infrastructure. The authors find a need for a methodology that can help developers create a more secure cloud architecture for healthcare services. The claim is that it is challenging to create this methodology because the infrastructure in healthcare environments is complex. Finally, Rizk et al. 2020 presents a result from the survey they have conducted. It contains evidence that the healthcare services do not have a reference guide to creating a secure IT architecture in the cloud. The authors also claim that the healthcare cloud architecture lacks the implementation of fundamental components. The study concludes with an emphasis that data should also satisfy requirements of accuracy, punctuality, and confidentiality.

Paul and Das 2018 concludes their study with a statement that expresses how medical services can take advantage of the new technology surrounding cloud computing. The authors claim that healthcare service providers can deploy more affordable medical services to their patients with the use of cloud computing. This claim relates to the effectiveness of the cloud and that each service provider can choose a custom infrastructure that fits them well.

Services utilizing cloud computing have many benefits for a healthcare service provider, with one interesting example provided by Chandrasekaran, Mohan, and Natarajan 2015: the provision of medication to patients without the need for patients to visit hospitals. The authors state that the major advantage of healthcare services in a cloud environment is that they can be accessed by either the patient or the healthcare service provider from anywhere in a short amount of time compared to older on-premises solutions. Highlighted key technologies are fast wide-area networks, powerful yet inexpensive servers, and high-performance virtualization for hardware. The study further explains that cloud computing advantages such as agility, reliability, portability, real-time, flexibility must be considered together with the fact that healthcare applications contain sensitive patient data. Meaning, this sensitive information should not be operated by any other traditional data storing systems. Chandrasekaran, Mohan, and Natarajan 2015 further identifies four important issues with cloud computing for healthcare:

- Security and privacy
- Data is more accessible by all users
- Disaster recovery
- Slow response times

The main challenges for integrating cloud computing and healthcare are security, Data Management, Design, Infrastructure, Service, and Deployment. However, the authors conclude by stating that if the necessary characteristics discussed in the article are implemented, then the cloud can provide a vast majority of positives, including greater storage spaces, unlimited access from everywhere, efficient sharing, better interoperability between providers (hospitals, doctors, and other medical organizations) as well as better disaster recovery.

The development in IoT and cloud computing-based healthcare applications from 2015 to 2019 was studied by Dang et al. 2019. They state that cloud computing is the new hot topic in the IT market because of benefits such as scalability, mobility, and security benefits by providing on-demand computing resources. The authors highlight the ability of cloud computing to enable sharing of information among health professionals, caregivers, and patients in a more structured and organized way. Finding that both IoT and cloud computing benefit healthcare services and applications.

According to Rajat Wason 2020 the rapid movement of cloud technology, as well as the increasing amount of sensitive data being processed in the cloud, is a big problem for some organizations. As stated by Mandal, Sarkar, and Chaki 2014 many healthcare organizations face a research challenge when it comes to the deployment of different services and applications that handle electronic health records in the cloud. Mandal, Sarkar, and Chaki 2014 also further explains that Healthcare organizations need to design better their cloud architecture, as well as their deployment of healthcare services. In other words, this means that healthcare organizations need a robust strategy when adopting their services to a cloud environment.

Griebel et al. 2015 finds in their survey of cloud computing in healthcare that there exist few successful implementations, and many of the papers in the survey "use the term *cloud* synonymously for *using virtual machines* or *web-based* with no described benefit of the cloud paradigm." Even though the survey is from 2015, it still highlights important issues for cloud adoption in healthcare regarding data safety and security.

Hurst et al. 2020 identifies distinct threat vectors that are specific to hospital critical infrastructures as: (i) dependence of legacy software; (ii) the vast levels of interconnected medical devices; (iii) the use of multiple bespoke software, and (iv) electronic devices (e.g., laptops and PCs) are often shared by multiple users. The study also highlights the trend of moving towards electronic patient record (EPR) systems, with over 83% of hospitals in the UK moving towards EPR at the time of the study.

Georgiou and Lambrinoudakis 2020 states in their study that cloud-based systems change the way we interact with information and that cloud-based systems offer great potential for the Healthcare IT sector. Cloud service adoption, however, greatly depends on several factors concerning data security and end-user privacy. The authors further explain that losing control when migrating a service to the cloud is a legitimate worry that many scientists have shared beforehand. Their study aims to provide a set of requirements to protect better healthcare organizations and patients that utilize cloud computing. The study uses the Confidentiality, Integrity, and Availability (CIA) triad as a part of the requirements that cloud computing security must comply with. They state that healthcare service providers have to deal with a comprehensive set of challenges other than cloud computing challenges. Examples provided by Georgiou and Lambrinoudakis 2020 are challenges regarding privacy, economics, accountability, as well as operational and technical security. The study defines a threat model, where the major threats are classified into the categories: identity and access management, data, regulatory, operational, and technology. Further, the study defines different threat scenarios that correspond to each of the categories. The authors then provide a list of potential mitigations for each of the threats.

Ouardi, Sekkaki, and Mammass 2017 investigates the Moroccan health sector and how the sector deals with increasing demands placed on healthcare providers. Even though the medical field utilizes an exponential number of data that requires a developed infrastructure and a very high storage and archiving capacity, which leads to slow processing of data and possible erroneous results. The authors propose an architecture capable of implementing all the information related to the ministry of health of Morocco to provide the Quality of Service (QoS) that the consumers expect. The study also mentions the use of a broker to enable the functionalities.

2.2 Cloud Security

2.2.1 What is Security?

Johnson and Easttom 2020 defines information systems security as "the act of protecting information and the systems that store and process it. This protection is against risks that would lead to unauthorized access, use, disclosure, disruption, modification, or destruction of information."

Peter Mell n.d. states that cybersecurity is referred to as a wide range of different capabilities, such as the ability to prevent threats and vulnerabilities from damaging computers and different electronic communication systems. The term damage is used similar to Johnson and Easttom 2020, that confidentiality, integrity, and availability together with authentication and non-repudiation are protected in electronic systems and computers.

von Solms and van Niekerk 2013 claim that cybersecurity extends its abilities in comparison to the common phrase *"information security"*. According to von Solms and van Niekerk 2013, cybersecurity is referring to the safety of human beings in addition to the protection of computer systems handling data. The authors explain that humans pose as potential targets for attacks such as social engineering, where attackers utilize the human mind to gain unauthorized access.

2.2.2 Security in a Cloud Environment

Cloud promises excellent benefits, but security concerns hamper widespread adoption according to Ali, Khan, and Vasilakos 2015. The number of users not related to the organizations is a significant concern, as the CSP might trust clients, but the clients might not trust each other. Also highlighted is the cloud characteristic of multi-tenancy and how this is promising for optimization of resource utilization at the same time as it poses a major threat to cloud environments. In their paper, Ali, Khan, and Vasilakos 2015 details the need for access control, identity management, the integration of assurance and auditing tools, and insider threat detection by judging malicious behavior as critical for cloud security strategies.

Important aspects of Cloud Security collected from Dotson 2019:

- Cloud asset management and protection - An important difference between cloud security and regular on-premises security is that the controls will be outsourced together with the cloud service itself.
- Identity and Access Management (IAM) - Access control and management in traditional IT infrastructure is often executed by physical access controls or network access controls. This approach is not viable in a cloud infrastructure as the organization neither has control over the physical access nor the complete network access controls.
- Vulnerability Management - Traditional vulnerability management processes are left behind in the rapidly evolving and innovative field of cloud computing. Hosting models in the cloud, such as containers or serverless hosts, make traditional vulnerability management tools.
- Network Security - The perimeter of traditional IT-based infrastructure located on the organization's premises is easily defined as it is feasible to model the network. In

cloud computing, however, the perimeters are not feasible to model for an organization, and the knowledge of what is inside the perimeter is dependent on the delivery model and CSP.

- Detecting, Responding to, and Recovering from Security Incidents - Worries that emerged for conventional IT environments was that the organization had to deal with everything happening in the given levels (Detect, respond to, recover from). The organization can migrate controls such as intrusion detection, incident response, and forensics to the cloud service provider for cloud computing.

Figure 2.2 displays findings from the Cloud Security Alliance (CSA) survey that examines the state of cloud security in organizations. The findings highlight that third-party solutions for network security are still increasing. However, the authors point towards organizations having difficulties implementing controls to meet the increase of cloud adoption due to Covid-19.

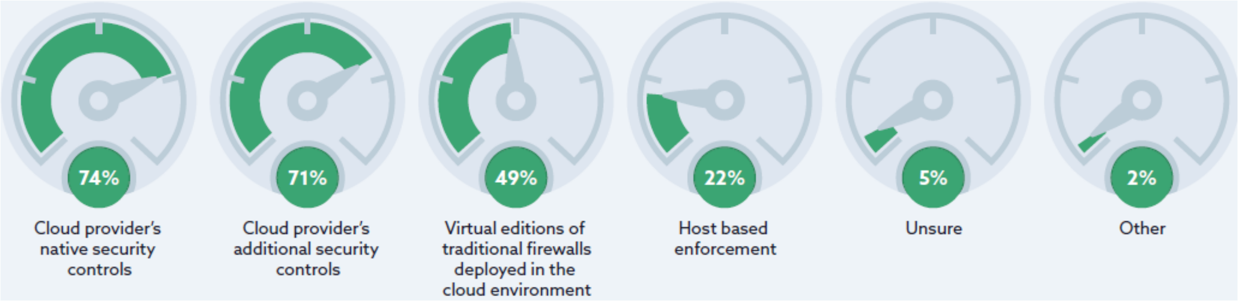


Figure 2.2: Security controls from the CSA survey Baron et al. 2021

The SANS 2021 Cloud Security Survey, displayed in figure 2.3, similarly finds that cloud computing and implementation of cloud security controls are increasing. The report's authors state that some of the standard security controls for cloud deployment are now available as Security-as-a-Service (SECaaS). The most popular SECaaS services in the survey are multifactor authentication, identity management, and cloud encryption or CASBs. However, findings also highlight that security controls are still managed internally, there is a growth in the use of CASBs and encryption gateways as a part of a growth in the use of hybrid computing, and that the numbers altogether are low. The SANS survey also finds that half of the respondents (51%) are leveraging security controls provided by the CSP.

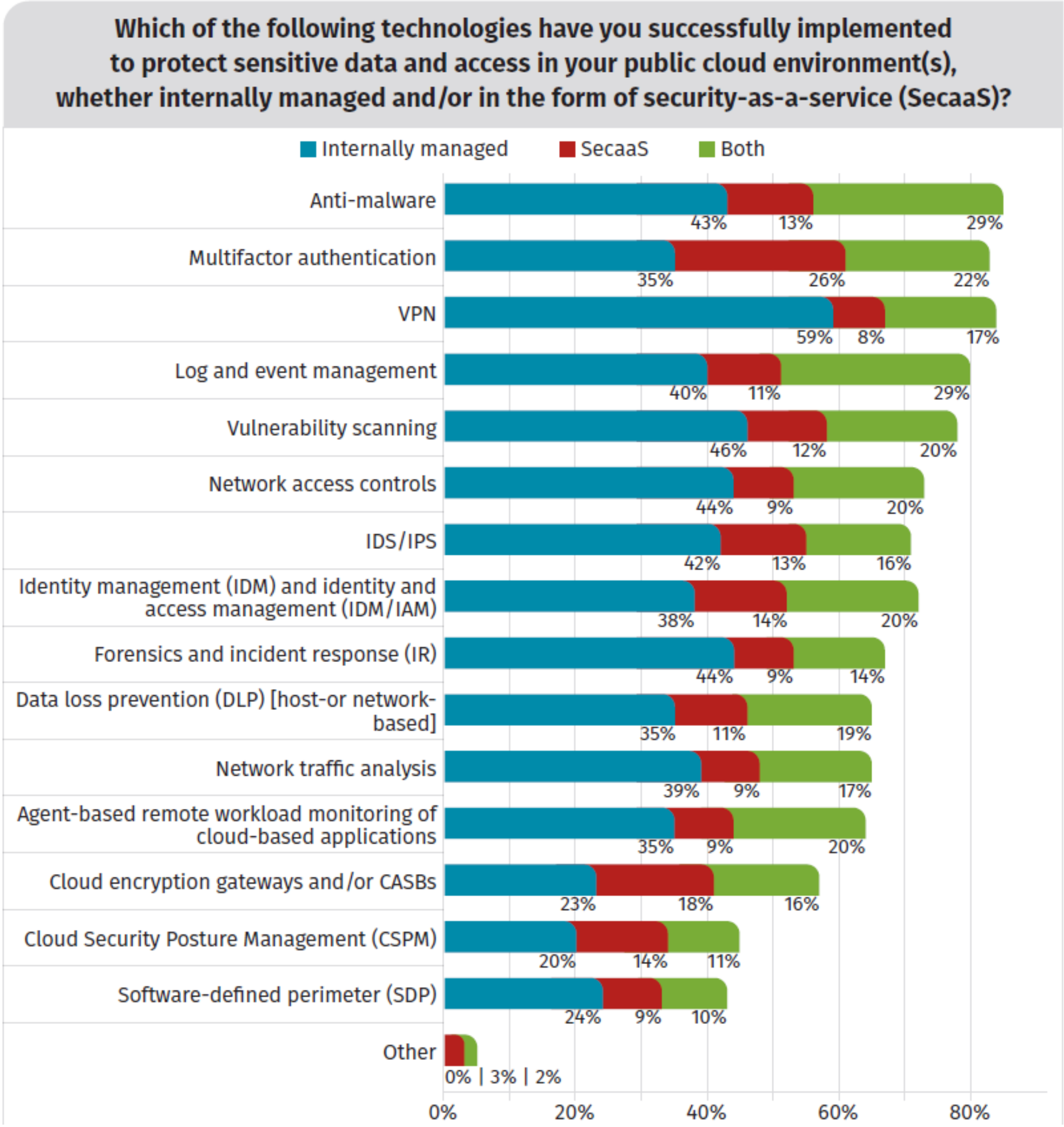


Figure 2.3: Organizational implementation of security controls, collected from the SANS 2021 cloud survey (Shackleford 2021)

2.3 Cloud Access Security Broker

Cloud Brokerage is a term used by Nair et al. 2011 in the description of a model that includes a Cloud Service Broker. They define a Cloud Service Broker as a platform that administers policies and secures the cloud environment by simplifying the complications of modern applications delivered by the cloud service providers. The platform is intended to be located between the provider and the consumer of the cloud services. In addition, it can also help enforce the correct IT policies. Nair et al. 2011 further proposes an architecture that focuses on secure brokering between multiple providers to provide a Service Level Agreement (SLA)-based tiered pricing model to the customers of the broker.

Elhabbash et al. 2019 states in their systematic survey that the cloud community has been claiming the need for an intermediary system between the customer and the Cloud Service Provider (CSP). The survey results show that the community wants a broker to mitigate the risk of selecting a CSP and that it can be the solution for the customer to find a more fitting service provider. The results also prove that intermediary solutions for the cloud can indicate different types of intermediation models. Elhabbash et al. 2019 uses the term to address the problem of a Cloud Service Customer (CSC) selecting a Cloud Service in a market with a high number of heterogeneous cloud offerings. The types of Cloud Brokerage models they describe are: Cloud federation, abstracting away the differences between CSPs, and a decision support system. The survey finds that the term "brokerage" was a term appearing as a model to select CSPs and is highly driven by the CSP's heterogeneity to satisfy customers. Several future avenues for cloud brokerage are also identified: Customer Assistance, Adaptive and Fluid Deployment, and Intelligent Decision-Making.

Obregon 2017 states in their SANS paper that unsanctioned applications in the cloud network that contain confidential organizational data are challenging in cloud computing. It is difficult for an IT security team to keep track of every user in the cloud network and what types of applications the employees utilize. Obregon 2017 also claims that it is harder for security professionals to affect the position of unsanctioned applications in the network since they do not have administrative control over these types of services. The author then refers to CASB as a potential solution to the problem. The four primary use cases for a CASB are identified as: Continuous Visibility, Compliance, Data Security, and Threat Protection.

Gartner n.d.(b) identifies a CASB as a security and policy enforcement point that is located between the customer and the CSP. CASB's core function is to incorporate security policies based on each organization's resources in their cloud environment. Gartner n.d.(b) also claims that a CASB can solidify different types of security policies within an organization, and examples of these are authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention, and so on. CASB has evolved to become a service offered by different companies, such as: McAfee MVISION (McAfee n.d.(b)), Symantec CloudSOC (Broadcom Inc. n.d.), Cisco Cloudlock (C. S. Inc. n.d.), Netskope Security Cloud (Netskope n.d.), Bitglass Cloud Access Security Broker (CASB) (Bitglass Inc. n.d.), and Microsoft Cloud App Security (MCAS) (Microsoft n.d.(a)).

In 2015 Gartner predicted that 85% of large enterprises would use a CASB by 2020, up from fewer than 5% at the time. Being so significant that the Cloud Security Alliance (CSA) picked up on this statement ((CSA) 2015). The report claims that "CASBs are a popular choice for cloud-using organizations." CASB is expected to continue to grow, with even higher growth than any other information security market at 33% in 2020 (Moore n.d.). According to Forbes (Columbus 2020), Gartner mentioned in their 4Q19 security spend forecast a prediction that "spending on Cloud Access Security Broker (CASB) solutions will grow 45.3% in 2020, 40.7% in 2021, 36.7% in 2022, and 33.2% in 2023, outpacing all other information security markets." According to Gartner n.d.(a), the CASB market is defined as "products and services that address security gaps in an organization's use of cloud services." With the technology being the result of the need to secure cloud services which again are being adopted at a significantly increased rate and access to them from users both within and outside the traditional enterprise perimeter, plus growing direct cloud-to-cloud access. In the same statement, Gartner also claims that CASB delivers services different from existing enterprise technologies such as web application firewalls (WAFs), secure web gateways (SWGs), and enterprise firewalls.

One of the essential functionalities CASB is advertised with is Shadow IT management. Shadow-IT, data loss, as well as data breaches, are some of the security challenges that are widely researched for cloud computing. According to Vandermarliere 2016, there are also multiple countermeasures that organizations can utilize in order to mitigate risk related to these issues. Cloud Access Security Broker (CASB) is mentioned as one of the more reliable security solutions for these security challenges specifically. From Vandermarliere 2016 's perspective, a broker between the cloud service provider and the enterprise is a potential solution in order to mitigate the risk related to Shadow-IT and data breaches. In addition, Vandermarliere 2016 indicated that more research is needed in order to test if CASB can address these challenges in the most effective way. In other words, an intermediary cloud service can solve some of the security issues and challenges related to organizations adopting the cloud environment. Rajat Wason 2020, further contributed to the research by developing a CASB implementation model on how organizations should deploy a broker system into their existing solutions.

Cloud components in enterprise architecture, and specifically in a healthcare service provider, needs complementing security controls to be viable. A CASB is an instantiation of a cloud security control that can complement existing cloud infrastructure. The CASB solution will function as an intermediary between the cloud customer and the cloud service provider, contributing to multiple security features and the on-premises security solutions already implemented.

2.4 Unified Threat Management

The idea of collecting several security technologies that can be used between a client and a CSP is used in other technologies. Gartner n.d.(d) defines Unified Threat Management (UTM) as devices that provide SMBs with multiple network security functions in a single appliance. Similarly, can multiple security features or services, when combined into a single device within a network, be referred to as a UTM, according to Fortinet n.d. Desired features of a UTM (Fortinet n.d.) is listed as: (1) Antivirus, (2) Anti-malware, (3) Firewall, (4) Intrusion Prevention with IDS and IPS, (5) Virtual Private Networking (VPN), (6) Web Filtering, and (7) Data Loss Prevention.

A competitor to UTM is the Next-Generation Firewall (NGFW), which according to Gartner n.d.(c) is a firewall that moves beyond port/protocol inspection to add "intelligence from outside the firewall." However, the NGFW technology is very similar to UTM, and it is argued that Gartner coins the NGFW term to sidestep the term UTM as UTM is initially a term originating from a Gartner competitor (Tam et al. 2013).

2.5 Cloud Security Control Decisions

Cloud computing is a new information technology paradigm, one which has been adopted in many different sectors (Al Mudawi, Beloff, and White 2019). An important aspect of this report is the government and public sector. Al Mudawi, Beloff, and White 2019 explores significant factors affecting the adoption of cloud computing in e-government services in Saudi Arabia as a case study. The authors then propose a model for the Adoption of Cloud Computing in Saudi Government (ACCE-GOV) based on the Technology Organization Environment (TOE) framework and the Diffusion of Innovations (DOI) theory. The study highlights factors in an organizational context (e.g., Top Management Support, Organizational Size, Technology Readiness), a technological context (e.g., Compatibility, Complexity, Service Quality, Relative Advantage, Security), an environmental context (e.g., Regulations, Competitive pressures), and a social context (e.g., Trust, Awareness, Attitude) as important factors for cloud adoption.

Existing studies on the selection of cloud vendors are mainly focused on technology and cost perspectives. Liu, Chan, and Ran 2016 argues that other influencing factors, such as competitive pressure, must be considered at the same time.

Organizations face many different factors when adopting cloud computing into their processes; it is, therefore, important that these factors are systematically evaluated before a decision on adoption is made. In their study, T. Oliveira, Thomas, and Espadanal 2014 assesses the determinants that influence the adoption of cloud computing by developing a research model based on innovation characteristics from the diffusion of innovation (DOI) theory and the technology-organization-environment (TOE) framework. They further state the importance of understanding the different elements of cloud computing and that it is significant for an organization to grasp it before they adapt to a cloud environment. According to the authors, some key elements are business process transformation and rapid application development. The results from the paper show that five factors will substantially determine the success of cloud adoption. From the paper, the five factors are:

- Relative Advantage
- Complexity
- Technological Readiness
- Top Management Support
- Firm Size

T. Oliveira, Thomas, and Espadanal 2014 concludes with the assumption that different sectors also have different drivers to consider, which further implies the importance of understanding cloud computing before adopting it.

The TOE framework is also utilized by Gutierrez, Boukrami, and Lumsden 2015 in their study on influences on managers' decisions to adopt cloud in the UK. They find that key factors influencing managers include competitive pressure, complexity, technology readiness, and trading partner pressure. The latter key factor: trading partner pressure, being the most significant of the factors and reflecting organizational concerns about legal regulations, co-creation and customization, service linkage, and vendor locking. The study also claims that one of the main drivers for cloud adoption is environmental factors. Authors state that the reason for this is how cloud computing has emerged as a key to business growth and that organizations accept the advantages of cloud computing to uphold business success.

Kissoon 2020 states that there is limited research in the area of information security decision making. Further findings suggest a need to enhance the decision-making process to reduce the number and type of breaches, even though the study demonstrates that organizations are actively implementing cybersecurity frameworks. The purpose of the study is to provide insight into the decision-making process used by organizations in cybersecurity investments through analysis of data collected from a pilot study. Organizations focus heavily on compliance with government and industry regulations and opportunity costs when investing in cybersecurity controls. The study indicates that decision-making can be biased when evaluating these new controls. The main reason is that the decision-making process is weighted towards technology and not other aspects. They are implying that the decision can be made based on wrong priorities. CIO and Head of the Business Line are also found to have similar priorities concerning funding the investment cost, implementing information security measures, and reviewing the risk appetite statement. If the viewpoints within the organization are different, then that may impact the decision-making when it comes to cybersecurity controls.

2.6 Decision Making on Security in Healthcare

Jackubczyk and Kaminiski 2017 motivates their study based on the complexity of decision problems encountered in health technology assessment (HTA). The authors seek to extend the model of evaluating the consequences of using health technologies by representing the suggestion a decision-maker considers as a stochastic multiple criteria optimization task. A typical suggestion consists of which technologies should be reimbursed or recommended for use in clinical practice. Preferences in HTA are best described using a fuzzy approach, the authors state.

Seixas, Dionne, and Mitton 2021 states that health systems have been pushed to improve decision-making practices on resource allocation due to growing expenditures. Therefore, the study is a scoping literature review that focuses on the practices of priority setting and resource allocation (PSRA) in healthcare systems residing in high-income countries. They identify three significant types of decision-making frameworks: 1) Program Budgeting and Marginal Analysis (PBMA); 2) Health Technology Assessment (HTA); and 3)

Multiple-criteria value assessment. Indications are found that point to the frameworks only being implemented in episodic exercises with poor follow-up and evaluation, further pointing towards a growing interest in explicit robust rationales and ample stakeholder involvement; however, this is not a norm. The study concludes that PSRA seemed to be the desired method, even though some elements were present in both designs. Some key process characteristics highlighted in the article was: A variety of stakeholders were involved in almost every case, several types of data were reported to inform decision making (e.g., published literature, clinical opinions, economic evaluations, HTAs, and data on disease prevalence), and approaches of willingness-to-pay thresholds are being abandoned in light of a greater understanding of the complexities of health care decision making, of the limitations of 'single truth' evidence and the need for broader stakeholder engagement.

Rajaeian, Cater-Steel, and Lane 2017 states that outsourcing of new technology is a common approach to maintain IT governance, and the claim from the authors is that it is a complex and difficult process. The literature review they present shows that a decision-making strategy can develop a better outcome for decision-making, but it is not that straightforward in practice. The authors explain that even though other researchers have come up with decision-making strategies, there is no complete analysis of that research. Most of the artifacts on decision-making follow a quantitative methodology, which can be problematic for real-life scenarios. Here Rajaeian, Cater-Steel, and Lane 2017 claim that there is a need for a design research and action research methodologies approach on this topic, which is more focused on the practical point of decision making.

2.7 Wicked Problems

Decisions in a real-life scenario of a security official in a large healthcare organization are complicated, and the process is convoluted. A decision on adopting cloud security controls for organizations, in general, is on its own a complicated matter as the solution space is unbound, and solutions are irreversible. These characteristics indicate that the adoption of cloud security controls for organizations is a wicked problem according to Rittel and Webber 1973. Initially defined to address problems in political science, wicked problems are defined by ten propositions (Rittel and Webber 1973): (1) There is no definitive formulation of a wicked problem. (2) Wicked problems have no stopping rule. (3) Solutions to wicked problems are not true-or-false, but good-or-bad. (4) There is no immediate and no ultimate test of a solution to a wicked problem. (5) Every solution to a wicked problem is a ’one-shot operation’; because there is no opportunity to learn by trial-and-error, every attempt counts significantly. (6) Wicked problems do not have an enumerable (or exhaustively desirable) set of potential solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan. (7) Every wicked problem is essentially unique. (8) Every wicked problem can be considered to be a symptom of another problem. (9) The existence of a discrepancy representing a wicked problem can be explained in numerous ways. The choice of explanation determines the nature of the problem’s resolution. (10) The planner has no right to be wrong.

Wicked problems are still relevant, and there is still interest in their nature and that answering the complexity can foster improvement (Crowley and Head 2017). Design theory consists of wicked problems, as "design has no special subject matter of its own apart from what a designer conceives it to be" according to Buchanan 1992. This aspect makes design problems "wicked" in nature. Design problems are potentially universal in scope, and the designer must adapt to the specific circumstances when applied (Buchanan 1992). However, Thienen, Meinel, and Nicolai 2014 states that design theory can help to solve wicked problems with tools and processes that take into account perspectives from different stakeholders. Kreuter et al. 2004 reiterates that in an environment with great uncertainty due to differences in perspectives of community stakeholders, a wicked problem is best resolved through a planned process with input from multiple sources.

2.8 Design Science

For information systems, it is important for practitioners to consider the technological aspects of information systems and the information that aids productive management and use of the information systems. Hevner et al. 2004 argues that to obtain such knowledge, one must involve behavioral science and design science. Behavioral science covers the organizational and human phenomena surrounding the analysis, design, implementation, management, and use of information systems. Thus informing of the interactions between the different parties (i.e., people, technology, and organizations). Design science is a problem-solving paradigm used to define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, management, and use of information systems can be effectively and efficiently accomplished (Hevner et al. 2004).

Chapter 3

Methodology

Chapter 3 will elaborate on the methodology chosen for this thesis and a justification of why this methodology was applied. Furthermore, the chapter will also describe the organization that we have been collaborating with and how literature was gathered to find evidence for the presented artifact that this methodology produces.

3.1 Action Design Research

Action design research (ADR) has been proposed as a tool for conducting an engaged form of research for advancing theory while producing useful knowledge. The method combines research traditions from action research and design science and focuses on designing artifacts that address a problem-solving environment and move together with the complex, ever-changing organizational context. ADR results in dynamic artifacts that can create value in a practical field such as elderly care. (Spagnoletti, Resca, and Sæbø 2015).

3.1.1 What is Action Design Research?

When designing an artifact for Information Systems, the artifact must be grounded in the theory that is applicable in practice. When conducting research, it is intuitive to base the work on existing theories. However, the world of Information Systems is complex, and the theory that someone has created might not work for others due to changes in the environment they work in. Therefore, it is important to include someone with practical experience when researching Information Systems and in the design of the artifact that is thought to solve the task. There is a conflict between what a practitioner needs to do their job versus what a researcher provides in methodical work to contribute academically. To bridge the gap between practitioners and researchers, a specific Design Research method was created. The method is Action Design Research and is created as a Design Research where the focus is to get feedback from practitioners in the process of creation Sein et al. 2011.

The ADR methodology consists of four different steps; firstly, the problem is formulated by identifying the classes of problems and the given research opportunity. The next step is creating the artifact, following the Building, Intervention, and Evaluation (BIE) model. In step three, the author reflects and learns from the interaction and identifies the contribution the project has to knowledge, research, and contribution to the organization. Finally, the last step is the formalization of learning, meaning the author should reflect on the accomplishments of the artifact, as well as what it has done for the organization Sein et al. 2011.

By involving an entire organization in the process, the ADR methodology makes it possible to evolve a created artifact with input from both the literature and the organization. Research can sometimes lack the input from the practical point of view, making ADR the ideal methodology for this thesis. Alternatively, one of the methods we could have used is an applied observational study. The applied observational study focuses on how a new solution fits into an organization's architecture, usually examined through multiple different conditions according to Edgar and Manz 2017. However, ADR is more focused on the coloration with an organization in practice, rather than simply observing the effects of a new security tool which is what we are looking to bring forward in this thesis. The applied observational study would not involve discussions and workshops to bring forward a result, which is more focused on collecting data through observation. With input from the authors of this paper regarding literature, in combination with the feedback from a real-life scenario, the artifact was shaped to become more relevant for organizations that require a cloud security control Sein et al. 2011.

An example of ADR application is the study of Spagnoletti, Resca, and Sæbø 2015, which uses ADR to focus on social media, and the contribution on elderly care assistance. In their paper, they motivate their work based on the need of more practically oriented research.

Artifacts

According to Hussain 2014, an artifact is an outcome of combining research data from multiple different sources. An artifact is an item or a component that is the result of applied research. In other words, the artifact in this thesis results from the combined knowledge of the researchers and the practitioners.

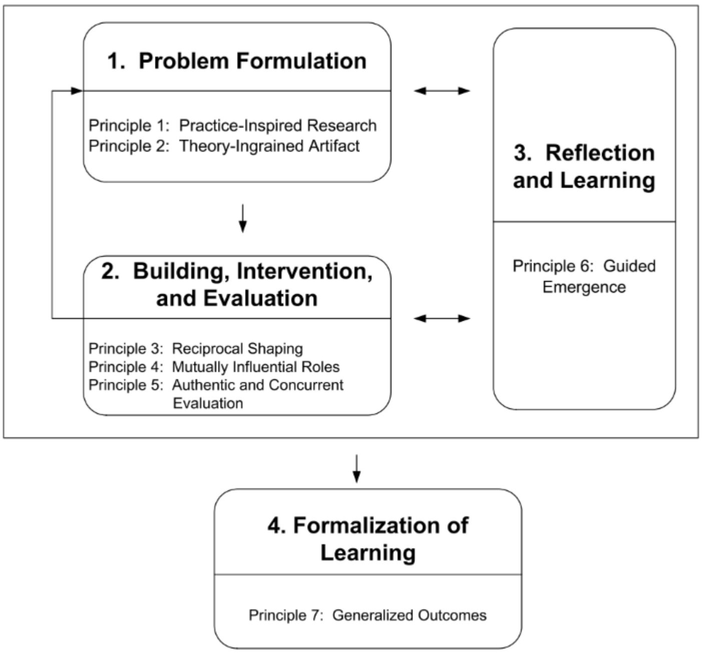

1. Problem Formulation
Principle 1: Practice-Inspired Research
Principle 2: Theory-Ingrained Artifact
2. Building, Intervention, and Evaluation
Principle 3: Reciprocal Shaping
Principle 4: Mutually Influential Roles
Principle 5: Authentic and Concurrent Evaluation
3. Reflection and Learning
Principle 6: Guided Emergence
4. Formalization of Learning
Principle 7: Generalized Outcomes

Figure 3.1: *This figure shows the ADR steps in correlation to each other*

3.1.2 Problem formulation

The problem formulation stage consists of six tasks that need to be in order before the researchers can build the desired artifact. Firstly the researchers identify the research opportunity, explaining why there is a need for research on the given area, followed by formulating the research questions. Then the problem is cast into an instance of the class of problems. In other words, the problem is formulated and reviewed within a bigger perspective. Instead of only solving the problem at hand, the artifact should look to see what it can contribute to solving other class problems. Finally, the researchers should plan a long-term organizational commitment in order to be able to perform the subsequent steps in the ADR method. By finding an organization that is willing to help the researchers, the artifact can take both inputs from the literature and a practical standpoint. The organization and the researchers form a team in which they collaborate to conduct the next step of ADR. For this thesis, the problem formulation step consisted of finding the initial problem at hand. By conducting interviews and meetings with an organization, the researchers determined the need for achieving a common understanding of new cloud security technology and support decision-making.

3.1.3 BIE Model

The next step is the Building, Intervention, and Evaluation model, where the artifact is formed through multiple cycles between the organization and the researchers. The team formed during the problem formulation step goes through the cycles presented in figure 3.2. Figure 3.2 shows the organizational dominant BIE model, which is one of two alternatives. The organizational model introduces the artifact to the practitioners early and focuses on challenging the organization's ideas and assumptions regarding the artifact. The other model is called IT-Dominant and is more heavily focused on the creation of a technological artifact.

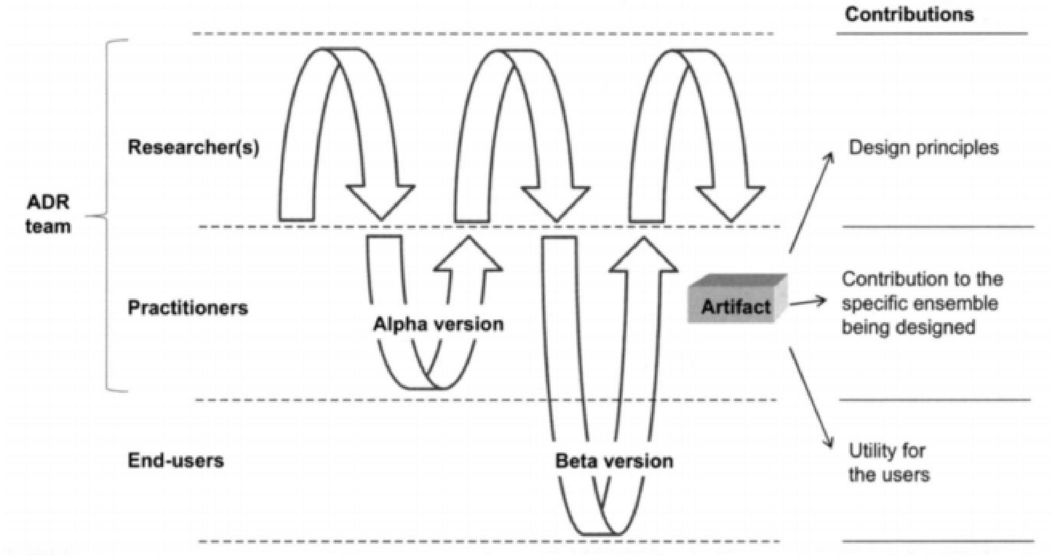


Figure 3.2: *The IT-dominant BIE model, Sein et al. 2011.*

The BIE model in this thesis consisted of cooperation with a healthcare organization in Norway. The researchers would perform the building, with input from multiple security experts within the organization provided as the intervention and evaluation steps.

3.1.4 Reflection and Learning

ADR encourages the researchers to apply what they have learned into the already created class of problems for the reflection and learning step. Instead of solving one problem at hand, the reflection and learning step will present how the artifact can solve multiple problems within the same domain of problems formulated in step one of the ADR methodology. Also, the way that the artifact contributes to research is documented during this step. The reflection and learning are meant to parallel the first two stages, as the learning from evaluation and feedback are used in the next cycle of the ADR process. Reflection should also highlight the increased understanding of the artifact that emerges during the research process. The most interesting feedback from the organization is presented so that the researchers can reflect on what they learned from it.

3.1.5 Formalization of Learning

Step four, formalization of learning, presents the outcomes that the organization is left with by the artifact. In addition, what the researchers learned from the process should also be developed into a more generalized solution for the given class of problems. The given outcomes for the organization are the design principles that the artifact has contributed to. During this step, the researchers derived a set of design principles that the artifact contributes to solving the organization. In addition, limitations, as well as future work, are also posed.

3.1.6 ADR-Team

During the problem formulation step, one of the tasks is to form an ADR team consisting of the people involved during the BIE cycles, which will be further elaborated on in a later chapter. However, in this thesis, we were able to work with a highly relevant organization to elaborate with practitioners from the field. The ADR team is a result of the collaboration with Sykehuspartner, and it consisted of the authors and two supervisors from the organization.

Sykehuspartner

The organization we collaborated with is Sykehuspartner, the largest supplier for healthcare ICT services in Norway. They host and manage ICT systems for every hospital within the South-East of Norway, which consists of ICT applications, ICT infrastructure, and network for 80 000 users Sykehuspartner n.d. Through the University of Agder, we got in contact with the CISO of Sykehuspartner and set up a problem formulation.

Sykehuspartner then provided two supervisors, helping us develop the artifact presented in this paper. These supervisors are security architects specialized in the field of the healthcare sector. In this thesis, a large organization refers to organizations with more than 50 000 employees as modeled in the SANS 2021 Cloud Security Survey (Shackleford 2021).

Gathering Data

In order to gather data for this thesis, the authors chose to conduct meetings and interviews with the organization. Sykehuspartner gave us the privilege of our own computer to have regular meetings with our supervisors and access the internal network as Sykehuspartner primarily utilizes sanctioned devices. Each interview was well documented to be able to go back and look at the data presented by Sykehuspartner. The interviews and meetings were all done through either Skype or Microsoft-Teams. Each meeting was planned through the mail, and occasional discussions and short messages happened through Signal. By organizing interviews with both the Computer Emergency Response Team (CERT) and the CISO, we were able to see the difference in perception of CASB internally in the organization.

Meetings and Interviews

The first two interviews were conducted with the CERT leader, which is the department that responds to information security threats within Sykehuspartner. The CERT is also monitoring and controlling the network for the healthcare sector covering the South-East part of Norway (Helse Sør-Øst). The South-East part of Norway is also the most densely populated part of the country. Due to many people and medical facilities, this specific CERT reports on the largest amount of security incidents and threats in Norway. In the first interview, questions were asked regarding the need for CASB and their vision for a CASB. These questions were asked to map and understand why Sykehuspartner wanted to know more about CASB as a security solution for the cloud. During the second interview, the researchers asked questions related to using cases of CASB. We wanted to know what their definition of CASB was and what they thought it would be able to solve within the organization.

The second interview was performed with the Chief Information Security Officer (CISO) of

Sykehuspartner. The CISO is in charge of acquiring new security solutions and managing every security decision within the organization. The interview guide contained similar questions to the ones given to the CERT leader. In addition to asking about the need for CASB, we also asked for information regarding their excising solutions and how they already handled security in the cloud today.

Finally, we had two interviews in collaboration with the Norwegian branch of Microsoft to fully understand the use case of a CASB and comprehend the features that their CASB could bring to an organization. Microsoft gave us a live demo of a CASB console to understand how to set policies and manage a CASB. We got to see how each cloud application is scored, and we got a live demo of a user account trying to break one of the added policies. For this interview, we presented our thesis to the professionals to discuss the different aspects of CASB with someone who had expert knowledge on the subject.

In addition to the interviews, regular meetings with our supervisors were conducted to ask questions and present our progression. In addition to interviews, meetings have been included as part of the BIE model because our supervisors brought constructive feedback throughout the whole process. Notes were taken during each meeting and were then later used to evaluate and outline the framework.

3.2 Framework Literature Methodology

The first step was to create a document to insert and sort all the relevant research articles found with various search terms. Next, articles were sorted into different categories to get an overview of the research and possibly get insight into where research is lacking. Finally, this overview was used to decide how our artifact should solve some of these research problems. The chosen areas of research were: framework-related research, research on key features of Cloud Access Security Broker (CASB), and relevant research problems in healthcare. Eventually, a table with these chosen articles was created to derive a class of problems related to each article chosen for each area.

3.2.1 Research on Frameworks

To start of articles regarding different types of frameworks were found, the reason is the desire to create our framework. In that regard, the strategy was to research frameworks related to topics within the cloud domain, security domain, and CASB. For the cloud domain, the authors wanted to find information on cybersecurity regarding how organizations move their business processes over to the cloud environment. On the other hand, the CASB area was chosen to find frameworks related to the implementation and deployment of CASB since the authors of this thesis wanted to know more about how well this was researched.

3.2.2 Key features of CASB

Furthermore, a collection of papers on the different key features of a CASB was gathered. This collection was done by looking at documentation from multiple vendors that offer a CASB solution. Both McAfee and Microsoft (McAfee n.d.(b); Microsoft n.d.(a)) were chosen since these companies are leading in the market when it comes to CASB solutions. The reason for researching these key features was because the authors of this paper wanted to know what a CASB solution could bring to an organization when it comes to security. Since as previously mentioned by Vandermarliere 2016, CASB was able to mitigate risk and solve security challenges severely. We wanted to know what types of measures CASB utilizes in order to solve these issues. Below is a set of key features chosen based on multiple vendors in the cloud business.

Key Feature	**Description**
Encryption	According to Kaur and Gupta 2019 implementing a CASB can help the organization establish encryption for all files that are uploaded to any cloud applications as well as files that are downloaded on unsanctioned endpoints in the cloud network. CASB can also block sensitive data from being printed, copied, or stored on endpoints as stated by Kaur and Gupta 2019. In addition, it is essential to note that encrypting all data in the cloud network can lead to latency issues and, in the worst-case crashing the cloud application.

Data Loss prevention policies	CASB DLP abilities can work together with existing DLP services within the organization. The difference is that the CASB will pick up traffic that also goes through the unsanctioned applications in the cloud network, meaning the applications that the regular DLP services do not detect as explained by Goel n.d. This difference is due to the deployment modes that CASB can implement, and reverse or forward proxy will give better insight into the unsanctioned application network flow. According to McAfee n.d.(a), the CASB DLP feature is to extend the on-premises DLP policies to also function within the cloud network. In addition, Microsoft n.d.(b) claims that a CASB can scan every file once it touches a cloud application, which means that a CASB can help better to detect DLP policy violations in the cloud environment.
Visibility and Shadow-IT	According to Microsoft n.d.(b), one of the use cases for CASB is to shed light on shadow-IT within an organization. A CASB can analyze the cloud network and determine what applications and services are used by which user account within the cloud network. A CASB can be deployed as a proxy, giving it full access to the cloud traffic, which means that it can detect unsanctioned applications that the organization does not have control over.
User Entity and Behaviour Analytics	According to Rajat Wason 2020 one of the security features that CASB offers is User and Entity Behaviour Analytics. The CASB can create a scoring system for every entity in the cloud environment by utilizing machine learning algorithms. Then each entity has a score based on their usual behavior, and the score will increase if that entity does a suspicious action.
Threat prevention	With all the abilities above in combination, the CASB can help existing threat prevention methods in succeeding. The CASB will offer UEBA, which can detect abnormalities and provide visibility over unsanctioned applications, which means it will be easier to implement threat prevention to detect threats earlier. This functionality can only work seamlessly if the CASB supports integration with the threat prevention security tool and vice versa.

Security Policies	According to Rajat Wason 2020 a CASB function as a broker between the customer and the cloud service provider, and one of the key features is to extend the organization's security policies into the cloud environment. The different security policies that a CASB can enforce are access control, encryption, device profiling, and many more explained by Rajat Wason 2020.

Table 3.1: *Table containing a set of CASB features*

3.2.3 Relevant Problems in Healthcare

In addition to papers on CASB and different frameworks, articles regarding problems in healthcare were derived from literature. As mentioned by Tervoort et al. 2020a, the healthcare sector is especially exposed to confidential personal identifiable information, which motivates malicious actors. Also, according to the same article, these breaches cost the industry billions of dollars every year. Therefore, the motive for this step was to investigate what types of security challenges these healthcare organizations face and the extent of these. Understanding these problems in detail would eventually create a more accurate framework based on modern problems that the healthcare sector is dealing with.

3.2.4 Defining Challenges

In order to be able to discover challenges related to the topics surrounding CASB, we had to derive papers from the literature. As many articles presented risk assessments on cloud computing, it was necessary to categorize all the established challenges.

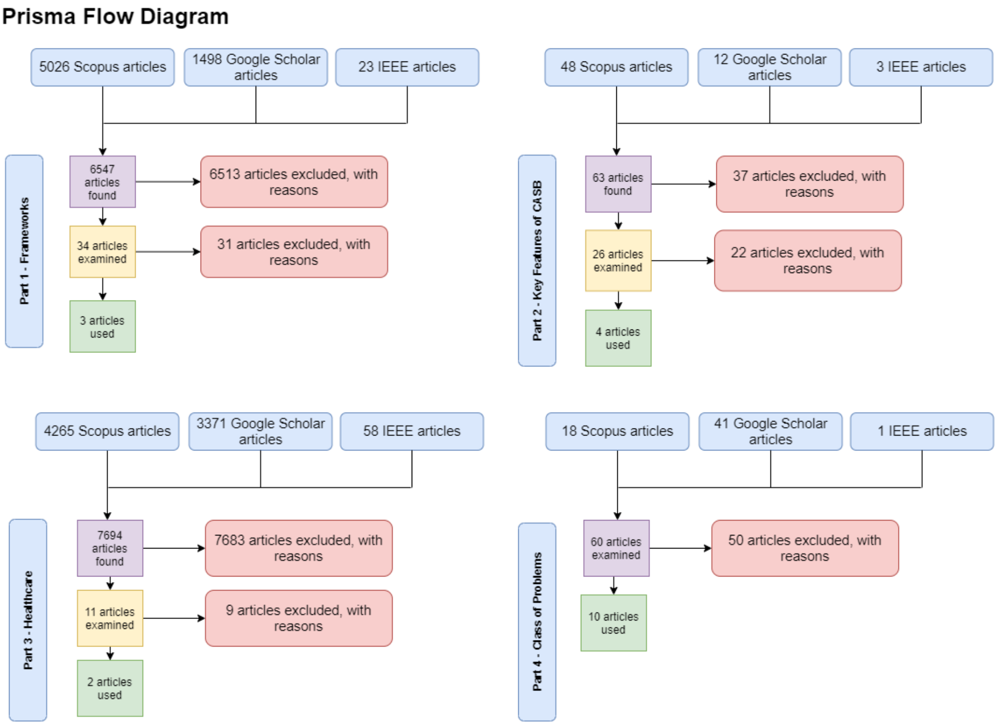

Prisma Flow Diagram
5026 Scopus articles
1498 Google Scholar articles
23 IEEE articles
6547 articles found
6513 articles excluded, with reasons
34 articles examined
31 articles excluded, with reasons
3 articles used
Part 1 - Frameworks
48 Scopus articles
12 Google Scholar articles
3 IEEE articles
63 articles found
37 articles excluded, with reasons
26 articles examined
22 articles excluded, with reasons
4 articles used
Part 2 - Key Features of CASB
4265 Scopus articles
3371 Google Scholar articles
58 IEEE articles
7694 articles found
7683 articles excluded, with reasons
11 articles examined
9 articles excluded, with reasons
2 articles used
Part 3 - Healthcare
18 Scopus articles
41 Google Scholar articles
1 IEEE articles
60 articles examined
50 articles excluded, with reasons
10 articles used
Part 4 - Class of Problems

Figure 3.3: *The Prisma Flow diagram for presenting the systematic literature methodology*

Figure 3.3 explains the methodology for the literature review using a Prisma Flow Diagram PRISMA n.d. For each part that was concocted for the literature review, new search terms were used to find information from different domains. For the articles on frameworks, 6513 articles were removed or excluded due to relevancy. Many of the search terms used, highlighted articles that were not relevant for the domains that are being researched in this thesis. The excluded articles contained information on, for example, physical security, rather than information security, or frameworks on on-premise security rather than cloud security solutions. Lastly, three articles were chosen and used in the final report, while 31 were excluded since the articles repeated the same information, meaning duplicate information was removed.

Articles on key features of CASB, 37 articles were excluded because these were writing about a different type of technology. Most of the articles did not cover the cloud perspective of the given key feature. The articles found could be related to encryption but contain a method for implementing a whole new cryptography scheme, which was not what we were after in this thesis.

Finally, research related to healthcare was identified. Seven thousand six hundred eighty-three articles were excluded because of the lack of information about the cloud environment in the healthcare sector. Most of the articles found contained information regarding Blockchain technology or the Internet of Things from a healthcare perspective, in other words, not relevant to the given problem at hand. The articles that were chosen to be included were relevant to either CASB, healthcare, challenges for cloud computing, or a combination of the three.

Chapter 4

Problem Formulation

The research opportunity and the initial research question are formulated during the problem formulation stage. By conducting meetings with Sykehuspartner, it was easier to establish what their current challenge was. In addition, the ADR team is formed during this step, and both the organization and researchers plan the steps going forward into the Building, Intervention, and Evaluation structure.

Through meetings, interviews, and discussions with Sykehuspartner, the initial problem was identified. Sykehuspartner has discussed the possibility of adopting CASB into their cloud architecture internally and has tried to implement parts of CASB as singular technologies (e.g., DLP). Through interviews, Sykehuspartner indicated that they wished for support on deciding if CASB was appropriate for them. Sykehuspartner will eventually join the quickly evolving field of cloud computing, and they wanted to be prepared more patient data being managed by cloud applications and services. Adopting a CASB seemed to be what competitors did, and they wanted to acquire the same measures that Gartner and different vendors advertised as the best solution for cloud security. This thesis is built around the observations that were conducted during the first weeks together with Sykehuspartner.

According to T. Oliveira, Thomas, and Espadanal 2014 one of the key elements of cloud adoption was to understand the technology at hand before deciding to adapt to it because of the rapid cloud application development that is in motion these days. Therefore we wanted to create a framework that could help Sykehuspartner decide if CASB was the proper cloud security solution. In addition, the framework was going to contribute to the understanding of the solution so that Sykehuspartner could better understand the technology before a decision can be made. Therefore, the problem is inside the category of decision-making on the adoption of a new security solution.

An important task for the problem formulation step is to identify classes of problems related to the defined problem, and the reason for this is to address the challenge at hand within a broader field. The class of problems our research question falls under is:

- *Decisions in public healthcare service provider*

The initial problem is that they could not justify adopting a CASB for their organization's cloud architecture. This problem will fall under the larger category related to decision-making for healthcare service providers. The intent for ADR is not to only solve the problem that Sykehuspartner has but rather utilize the formulated knowledge and apply it to a class of problems. This is the Acton Design Researchers contribution to literature according to Sein et al. 2011.

The defined class of problems instantiates what has been previously defined in literature as a *wicked problem* (Rittel and Webber 1973). A wicked problem is defined as a problem context that is poorly formulated, confusing, and permeated with conflicting values of many decision-makers or other stakeholders. Decisions in a public healthcare service provider are complex, with many decision-makers and stakeholders with conflicting values. The decision-making in this scenario is an unstructured process strongly influenced by the biases and background of the decision-makers and stakeholders. The defined class of problems is confusing and will therefore produce obscure results. This notion of obscurity speaks to the inherent uncertainty in such problems. Pries-Heje and Baskerville 2008 further mentions that organizational decision-makers face problems of such nature in an increasing amount.

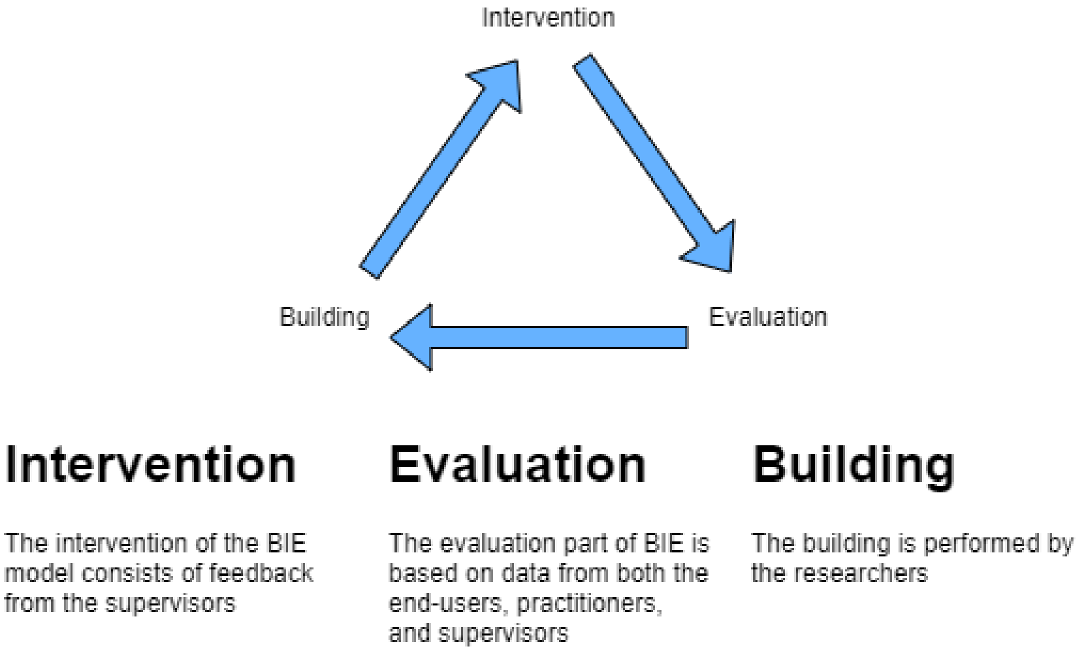
An agreement was made between the practitioners and the researchers that they were to conduct regular meetings where the framework was to be discussed and improved. The researchers were going to use the feedback and input from the practitioners to structure and scope the framework into an artifact that was usable for an organization and solving the problem at hand. In other words, a framework that could help Sykehuspartner decide on CASB while also providing more information on the subject.

Chapter 5

Building, Intervention and Evaluation Model

Chapter 5 reflects how the framework was built using the previous chapter's presented Action Design Research methodology. This chapter highlights the BIE model and how the artifact was shaped using the IT-dominant BIE model cycles by conducting regular meetings with Sykehuspartner and collecting data. Each version of the framework is presented and explained in detail in this chapter.

The second step of the ADR methodology is focused on building and evaluating the artifact. For this stage, the artifact is formed using multiple design cycles, where the ADR team combines their knowledge to create a tailor-made version of the artifact better. There are two types of design cycle BIE models in the ADR methodology: the IT-dominant and the Organizational-dominant BIE. For this thesis, the IT-dominant model was more suited, mainly because the end-users were not involved until the final workshop, which follows the structure of the IT-dominant design.



Intervention

The intervention of the BIE model consists of feedback from the supervisors

Evaluation

The evaluation part of BIE is based on data from both the end-users, practitioners, and supervisors

Building

The building is performed by the researchers

Figure 5.1: *Overview of the participants in the BIE model, and which people that were involved in each step.*

Figure 3.2 refers to how the BIE cycles were executed. First, the researchers did the building process of the artifact before the artifact was taken into the intervention and evaluation part through practitioners and end-users. These steps were then repeated until the artifact was complete. During the ***Building*** step, the artifact was influenced by literature and theory while considering the given feedback from both the evaluation and the intervention steps, which was conducted by the researchers alone. In the ***intervention*** step, the researchers were in discussion with the supervisors provided by Sykehuspartner. The supervisors were cloud security professionals and had a broad knowledge of cybersecurity and security architecture. Finally, the ***Evaluation*** step consisted of the collaboration with both the end-users, researchers, and the practitioners. This was the step where the artifact was shown to the employees that were going to utilize this artifact after the final process, in other words, the CISO and the CERT.

5.1 Groundwork for the Framework

As seen in figure 3.2, the IT-dominant model has multiple cycles in which the artifact is formed. For the first cycle, the framework was based on theory found by reviewing papers in the literature. By evaluating the state of the art, multiple articles and papers regarding CASB and healthcare were considered when creating the framework. The artifact was, at that time, solely based on input from the researchers. From the evaluation of literature, the researchers found articles related to the use cases and features of a CASB in table 3.1. First, the most important features were chosen from the list, and then the researchers created a need-analysis regarding each one. The chosen features were:

- Access Control
- Encryption and Key Management
- Shadow-IT
- Firewall
- Threat Prevention
- Security Policies
- Logging
- IDS/IPS

Each feature was described in detail regarding what it was and why it was important for the organization. The questions were found through papers on CASB and information from each vendor providing CASB as a solution. Three of the biggest vendors were chosen in order to compare CASB capabilities and create relevant questions for mapping the need for CASB: Microsoft, McAfee, and Netskope. For example, one of the vendors stated that CASB had a new Adaptive Access control feature. Then one of the chosen questions for the framework was: *"Does the organization have adaptive access control (AAC)?"*. In addition, for each question, the researchers tried to add a requirement. For example, a requirement belonging to the previous example was: *"The acquired CASB solution shall provide the organization with Adaptive Access Control (AAC)"*. Adaptive access control is a feature that CASB has, meaning the access control is performed dynamically based on each user's score in the cloud network. If the user has a higher risk score, the system will threaten access control differently rather than for a user that has a lower score.

5.2 First Draft of the Framework

Furthermore, the framework's foundation was presented to the practitioners and changed based on their feedback, which created the first draft. This feedback was the first interaction with the practitioners, and it formed the framework in greater detail. Sykehuspartner came up with several ideas that were not considered during the first theory ingrained cycle. Their view was different from the research since they had routines for interacting with new security measures. Sykehuspartner was more focused on the risk of implementing a CASB solution, and instead of seeing only the positive sides of a new security solution, they wanted to know what measures a CASB was meant to replace. In other words, the practitioners were more critical to a new security solution than what the researchers were during the first cycle.

The initial framework's intent was to act as a need-analysis, with questions leading up to the need for CASB for them to create a set of demands related to the answer to these questions. The practitioners thought the idea of creating a need analysis was something they could make use of; however, they argued that creating demands was not an easy task. Many employees had created demands from former assignments and stated that this was a tedious task and could take years of practice to get correctly. They suggested editing these demands out of the framework.

Together, the BIE group agreed that the first draft should include a scoring system in addition to the need analysis and remove the part containing demands. Eventually, the first draft consisted of questions regarding Sykehuspartner's needs for CASB and a score, based on what the practitioners would answer to these questions. The researchers wanted to present the result more clearly, so they utilized a radar diagram to pose the results from the scores.
Figure 5.2 represents one of the first radar diagrams that were presented for Sykehuspartner. The main point of the diagram was to show where Sykehuspartner was lacking when it comes to cloud security, based on CASB functionality. The numbers presented in the figure are all fictional, based on an example made to show Sykehuspartner. Altogether, this was the first draft of the framework presented in this thesis.

The researchers utilized the given feedback from the practitioners and went back to the literature to improve the framework - this time with a different type of focus. Instead of researching how CASB could solve problems, the researchers tried to find articles defining

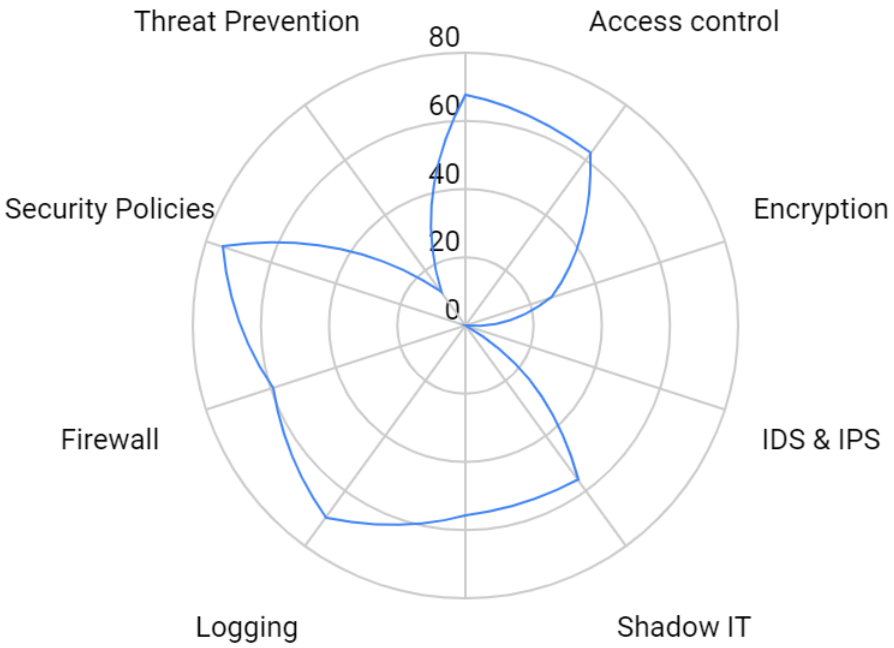


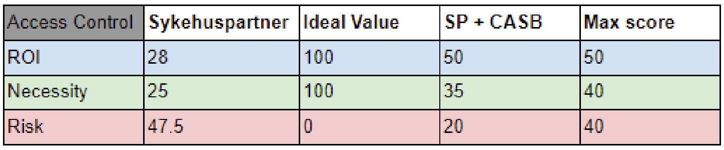
Figure 5.2: *Shows the radar diagram from the first draft of the framework*

CASB and negative sides regarding the implementation of CASB. During the research, some articles regarding the definition of CASB were found. For example, according to Twum, B., and K. 2020 CASB is a proxy that will filter through the data in transit, and that it can monitor all data transactions in the organization's network. In addition, Twum, B., and K. 2020 explains that CASB is a part of the Security as a Service solution and can be defined as a platform that the customer acquires in combination with other security measures. In another article, Han et al. 2020 stated that one of the downsides with a CASB was that it has to adopt each cloud application and reverse engineer the network protocol, which can be time-consuming and labor-intensive.

5.3 Second Draft of the Framework

Before the researchers were done with the next literature step during the BIE-model, an intervention was made to narrow the field of the framework down. Instead of looking at multiple categories for CASB, the researchers wanted to scope it only to become the most important ones for Sykehuspartner. Research towards that many categories concerning CASB was too much to put into a framework of this size. The researchers decided to only focus on three main categories that they thought suited the need of Sykehuspartner the most; Access Control, User and Entity Behaviour Analytics (UEBA), and Shadow-IT. The choice was based on Sykehuspartner's reaction to the meeting, and interviews were done before this step.

Other aspects were changed as well; at this point, the scoring system was based on three main categories: Return of Investment, Risk, and Necessity for CASB. By having trouble scoring the previous questions, the researchers wanted to go back to previous statements from Sykehuspartner that they wanted to acknowledge the return of investment (ROI) from a CASB and the risk related to the implementation of the new security solution. In order to present all this into the framework, the researchers utilized the same radar diagram from the previous draft. However, this time, it was focused only on ROI, Risk, and the necessity for CASB.



Access Control	Sykehuspartner	Ideal Value	SP + CASB	Max score
ROI	28	100	50	50
Necessity	25	100	35	40
Risk	47.5	0	20	40

Figure 5.3: *Scores on Access Control, based on a fictional business case.*

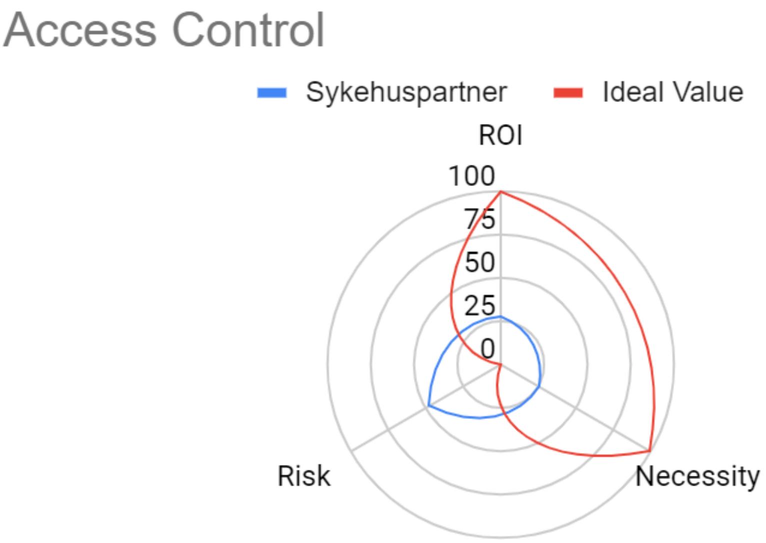


Figure 5.4: *Second draft radar diagram based on the scores from 5.3.*

Figure 5.4 represents the radar diagram for the second draft of the framework, and it contains scores based on what was answered in the framework. Questions here were based on the existing solution for access control, the cost of implementing a CASB. The following scores are based on fictional numbers made up by the researchers in order to justify a point for Sykehuspartner and see if the framework was working as intended.

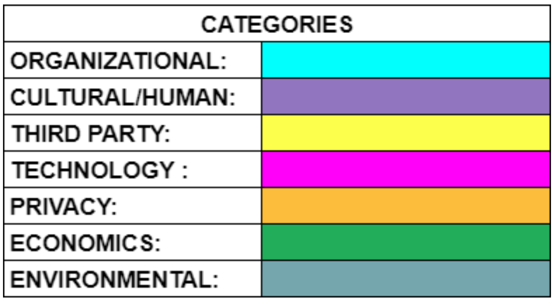
5.4 Final Draft of the Framework

The second draft was then presented to the practitioners in the BIE team. Sykehuspartner had constructive and valuable feedback towards important changes during this step in the BIE model. First of all, they explained the complexity of presenting risk, ROI, or necessity as a single integer score. These aspects need to be reviewed from multiple angles, and can change dependently on other factors, and are complex to measure. A discussion was made to change the framework completely, and instead of presenting need, risk and ROI, the framework could be utilized as a decision framework instead. So by going back to the drawing board, the researchers decided that it was more valuable to utilize a set of challenges specific to the organization. Then, the analysis would present three filters that would describe in detail how CASB's abilities can help the organization deal with these challenges. Finally, the researchers and practitioners decided that the framework also needs an evaluation in the end or a comparison.

The framework we have ended up with is thought to foster constructive discussion around how the different challenges are best solved for the organization. A detailed overview of all Cloud Assets can be a helpful addition to the framework. A tool for discussion will be of more value to a large organization, as creating a detailed overview of the cloud ecosystem and every control document is too time-consuming to justify.

From this standpoint, the framework could be used in order to decide if CASB was the right fit to the organization by presenting a set of challenges related to cloud computing, for then to compare the challenges with the CASB aspects of Access Control, UEBA, and Shadow-IT to filter out if the CASB aspects, could positively impact these challenges. If yes, then the scale would tip in favor of implementing CASB, and opposite if the challenges could not be solved. Therefore, a support decision framework was more valuable for Sykehuspartner rather than a need analysis, as previously presented. Sykehuspartner already had good routines for performing risk-and vulnerability analysis. In addition, the radar diagrams did not understandably present the values because it is not very useful to compare ideal values to practical values. The ideal values would always be either 100% or 0% since the organization would always wish to have the return of investment at 100% when implementing new security measures, as well as having risk at 0%.

By identifying different challenges related to the cloud for the organization, it is possible to filter out what CASB can solve as well as not be able to solve. Each challenge is categorized with a given color, and the categories in figure 5.5 are the first categories that were implemented.



CATEGORIES	
ORGANIZATIONAL:	🟦
CULTURAL/HUMAN:	🟪
THIRD PARTY:	🟨
TECHNOLOGY :	🟥
PRIVACY:	🟧
ECONOMICS:	🟩
ENVIRONMENTAL:	🟦

Figure 5.5: *Categories for each challenge, presented with a color pallet*

The business driver-category represents challenges that are related to what the organization strives for. In Sykehuspartner's case, a business driver example is to save lives rather than maintain security on the highest level. The risk category is related to challenges that pose as a potential risk for the organization, for example, shadow-IT. Shadow-IT is not directly a problem but can be a critical risk factor for the organization. The Cultural/Human category refers to human error and can be related to the challenge of security misconfiguration. Third-party challenges are related to outsourcing, meaning that another service provider makes a mistake that can impact the organization. Finally, the technical category contains challenges related to a technical mistake, vulnerability, exploit, or even a bug. Examples of challenges related to this category are insecure interfaces and APIs (All the examples above are explained more in-depth during the business case).

After each challenge is identified, they go through each of the chosen CASB technologies, represented as multiple filters. In this case, the filters are Access control, UEBA, and shadow-IT, which were chosen with respect to the feedback from Sykehuspartner. For every filter, the organization discusses if CASB's Access Control, UEBA, or Shadow-IT abilities can help to solve the identified challenges from earlier.

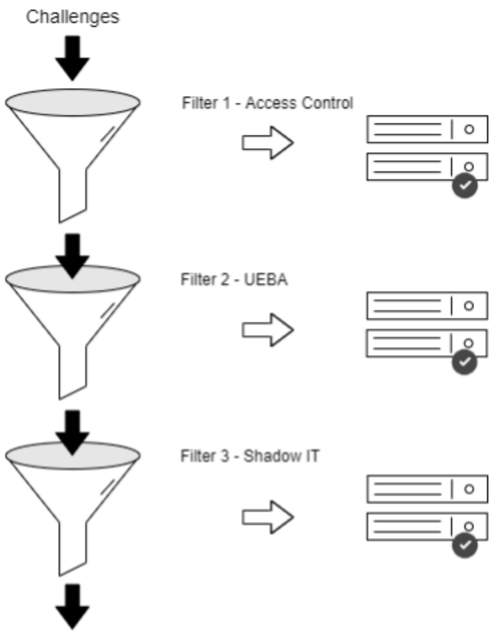
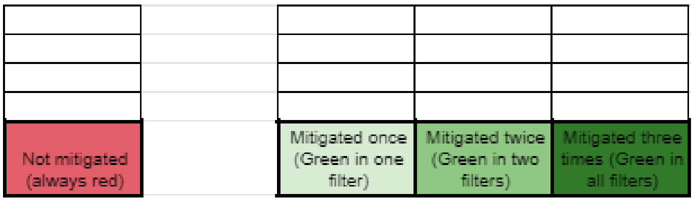


Figure 5.6: *Each applied filter for the final version of the framework*

As seen in figure 5.6, each filter will showcase which challenges might be positively impacted by the implementation of a CASB and which ones do not. One challenge might be positively impacted multiple times, but that will only make it easier to argue that CASB is worth it during the final discussion and comparison step. Finally, after each filter has been applied, the final step is to discuss and compare the results. Note that each challenge might weigh differently, and it is important to identify which challenge the organization feels is the most important to solve. One challenge might, in the worst-case scenario, outweigh every other challenge identified. Every challenge is then put into a category of how many of the filters caught the specific challenge.



Not mitigated (always red)		Mitigated once (Green in one filter)	Mitigated twice (Green in two filters)	Mitigated three times (Green in all filters)

Figure 5.7: *Final comparison for the decision framework*

The blank rows from figure 5.8 are where the organization fills in the challenges that have been identified. If most of the challenges fall under the "Not mitigated" category, then the reason for acquiring a CASB might be non-existent. On the contrary, if most of the challenges fall under the "Mitigated three times" category, one might argue the opposite.

Further explanation of the different parts of the framework is found in the Decision

Support Framework Guide document attached in appendix A. The Guide walks participants through the process to evaluate the impact of the security control in question.

5.4.1 Evaluation and Workshop

In order to make decisions on new technology, an organization should know exactly what the new technology is capable of, as well as the risk related to implementing it. For Sykehuspartner, there were multiple people involved in making a decision and carrying out detailed risk assessments for new technology. However, there seemed to still be difficulty in deciding if the technology was appropriate, and since so many people were involved, different opinions emerged. On the one hand, the CISO stated that the lack of a common definition of the security features included in a CASB solution made him uncertain that CASB would be the overall best solution for cloud security.

On the other hand, the CERT was convinced that CASB was a technology they indeed had to acquire in order to mitigate challenges related to cloud adoption/migration. Even though the return of investment indicates a reduced profit, the security might increase. The return of investment might not show the complete picture; however, there is no doubt that CASB will increase security in the cloud. In other words, that is enough evidence for the CERT team to argue that this indeed a security tool that Sykehuspartner needs.

Opinions on CASB	
CISO	*CERT*
Feels that the existing solutions are sufficient enough to secure the organization from cloud threats & Wants CASB functionalities since it can support existing security solutions in adopting cloud computing	Wants CASB functionalities since it can support existing security solutions in adopting cloud computing
Indicate that the challenge regarding Shadow-IT is not a threat that the organization need to solve yet	Argue that CASB can solve the challenge related to Shadow-IT for the organization
Argued that organizations developing specific security measures must be a more reliable solution rather than what CASB provides	Do not think Splunk is sufficient enough for all the cloud traffic and that CASBcan be a potential solution to handle all the data

Table 5.1: *Explains the different views of CASB as a security solution from a CISO and a CERT perspective*

In every organization, there will always be different opinions and different interpretations of new security technology. In addition to the different views of the CISO and the CERT, security advisors within the organization also have different opinions and knowledge on the given security solution. In other words, the security advisors can also contribute towards influencing the CISO and the CERT opinions by providing them with knowledge or impressions on the security technology. Security professionals who favor acquiring a new security technology can sometimes lose sight of how the new security solution is supposed to be operated and administered over time. It is important to note that security solutions can have a big impact on the organization's data since it is often given considerable flexibility in a network. This impact applies especially to CASB since it collects an extensive amount of data that is used for behavior analytics and other detection methods. Therefore, security personnel must understand the extent of the security technology and how it should be administered over time.

This mindset is where evaluation is important in order to make a proper decision. With the current artifact presented, it is possible to create a detailed evaluation of the new technology at hand. In our case, it is presented with CASB in mind for the selected filters. So each filter will explain to the users how the given CASB ability is defined and which of the selected challenges it will solve. By doing this, both parties involved in the decision-making will be able to debate if the new security solution in the cloud is correct based on evaluating both what it can solve and what it cannot solve.

By conducting a final workshop with the practitioners and the end-users of this artifact, we discovered that there were conflicting views on CASB. The workshop involved representatives from the CERT, the CISO, and other professionals from the security team. Together we went through the final version of the framework step by step, filling out both challenges and how they felt that the filters addressed the given challenge. Finally, we discussed the comparison of the challenges and how they were filtered in the hopes of giving the end-user a clear understanding of CASB.

This workshop created multiple discussions on the aspects of CASB and the presented risk and challenges towards Sykehuspartner. As presented in Table 5.1, the visions of CASB were different within Sykehuspartner. This created a valuable discussion on creating a common understanding for adopting new cloud security technology. Each participant in the workshop had the option to express their opinions and create a discussion on both the positive and negative sides of CASB. We noted that it is particularly important to involve different security professionals from different backgrounds when deciding if new security controls should be implemented or not. By conducting a workshop utilizing a decision support framework, it was easier to understand the definition or give a sense of the security technology being selected and create discussions with different points of view towards cloud security. If CISO was going to decide himself, the artifact might not be implemented at all because, from a financial point of view, CASB is not worth it. On the other hand, if the CERT were to decide, they would invest in a CASB without a doubt since they are more focused on the technology aspect of creating a more secure cloud environment.

Cloud Security Alliance Top Threats

Another evaluation provided to the framework through the workshop was to implement collaboration with another framework such as Cloud Security Alliance (CSA) top cloud threats. The suggestion was to create a set of general challenges that would be a part of the framework, regardless of whom was assessing it, based on CSA's top 11 cloud computing threats. CSA has provided a list of threats that are considered the most relevant. The list is based on a survey conducted in association with 241 security experts on challenges related to cloud computing from different organizations. The following eleven threats as presented by Alliance 2020 are listed below.

1. Data Breaches
2. Misconfiguration and inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking
6. Inside Threat
7. Insecure Interfaces and API's

8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services

5.4.2 Framework Filters

Each filter in the final version of the framework represents a feature that CASB offers. If an organization utilizes this framework, then they can choose to add other filters as well in order to suit their business needs better. Access Control, UEBA, and shadow-IT are set as the scope for this thesis.

Access Control

According to Atlam et al. 2020 access control is the ability to limit the actions that are performed by users in a network, as well as maintaining the security demands of confidentiality, integrity, and availability. Access control is not the same as authentication or authorization. Authentication is defined by the identity of a user, while authorization is the option to block or allow a user to perform a certain type of action. Atlam et al. 2020 identifies access control as the process of creating policies that are related to authorization. Firstly the user is identified (*authentication*), then it receives a level of privileges (*authorization*). Finally, the access control policies are meant to act as permissions for the user not to access anything outside of their scope. Examples of this scope can be accessing files that the user is not privileged to access or if the user has access to a specific place in the network that they should not.

CASB will contribute to delivering policies for access control for unsanctioned applications and devices in the cloud network. Usually, the unsanctioned devices do not go through the implemented access control. Since CASB can discover these devices, then it can provide access control policies for them as well.

CASB also utilizes adaptive access control, which is a type of access control that has been fed a context and balances the level of trust against risk when creating the policies, according to Wells 2020. Even though a user has the right credentials, it is not always safe to provide that user with access to a certain application. Adaptive access control usually needs input in order to create the correct context, and this is where CASB comes into play by providing a scoring system for each device in the cloud network. In other words, the CASB will update the access control policies in real-time based on for example, where the user is logged in from, the security score of that given user, or what type of device the user is on.

According to Kaur and Gupta 2019 a CASB will enable an organization to define individual policies by each application in the cloud network, and on top of that, control functionality within an application. CASB's access control can categorize the roles of each employee in the cloud network. For example, the CERT is the only team to access certain important files. It will also detect if there is any change in geolocation, for example, if a cloud user does an impossible travel. Meaning, the user logged in from a country, then logged in from another country in a couple of minutes in which it was impossible for that person to travel physically. Another aspect of CASB access control, according to Kaur and Gupta 2019 is the ability to set policies in real-time based on the device that the user logs in from. Many organizations have policies based on corporate-managed laptops, but CASB access control will also pick up if a user utilizes personal mobile phones in the cloud network.

In order to see the reason for choosing CASB access control, one has to look at the CASB as a platform that can contribute to making the existing solution better and not replace them. For access control, CASB might bring new features to the existing solution in order to improve access control and not replace it.

User and Entity Behaviour Analytics

User and Entity Behaviour Analytics (UEBA) is a way of using analytics to discover threats in a network according to CipherCloud 2020. This analysis is based on collected logs and alerts and is eventually creating a behavior profile on each entity in the network. In that way, the system that is utilizing UEBA will be able to detect abnormalities in the network based on how each profile is behaving. This is often combined with machine learning in order to make the analysis more accurate, as explained by Microsoft 2020. An entity can be a host, a user, or an application in the organization's network.

UEBA can significantly improve the organization's incident management. Not only will it allow for better tracking of user traffic, but it will also help the organization detect insider threats early. UEBA will also help with analyzing every user account's actions. This can range from downloads or simply what is being shared between users. Every organization needs this in its cloud environment in order to keep security up-to-date. Below is a figure that represents the three pillars of CASB as presented by Gartner 2020 in their 2018 market guide for CASB.

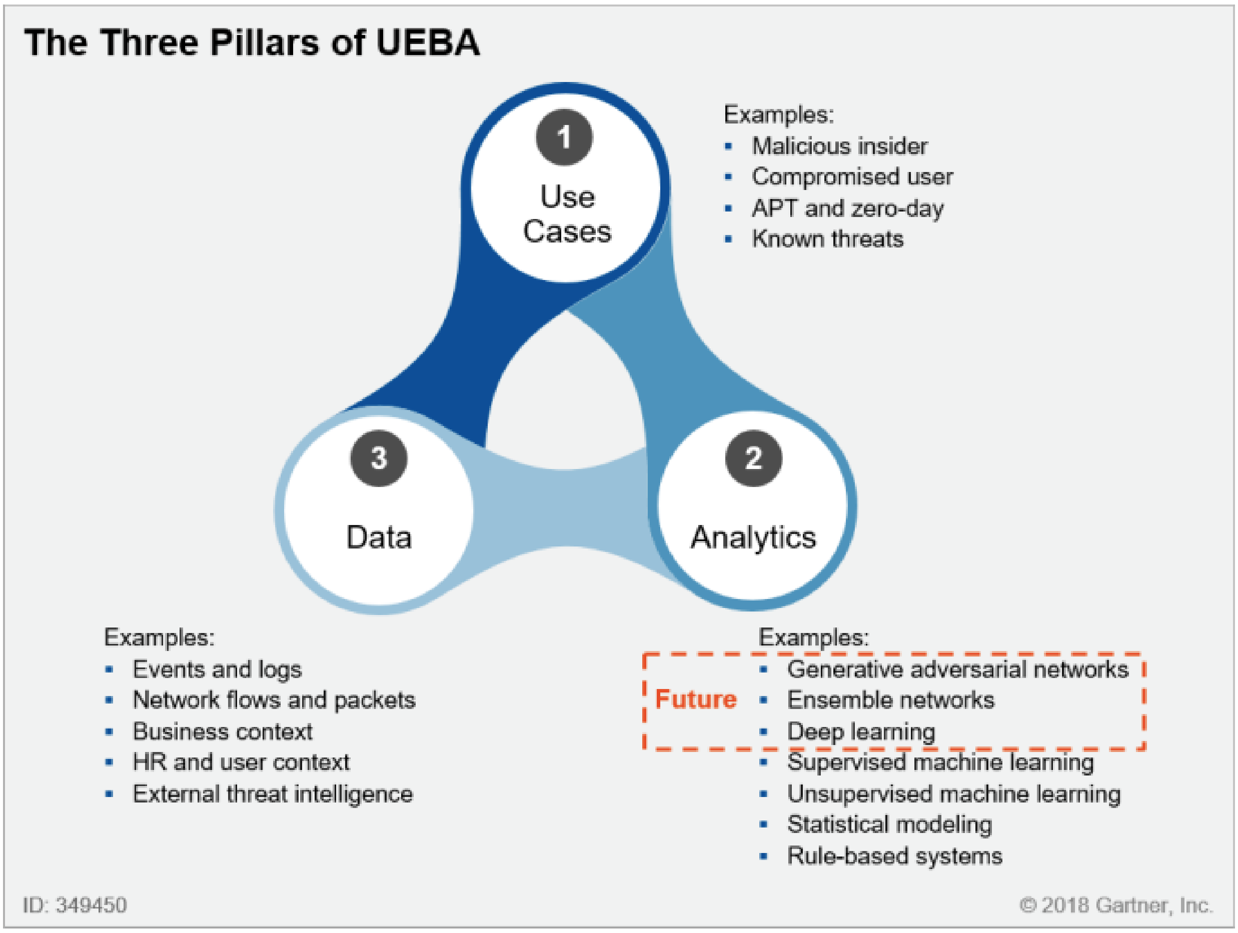


Figure 5.8: *The three pillars of User and Entity Behaviour Analytics as presented by Gartner 2020*

An example of use cases according to **fig:ueba_pillars** is inside threats, where the threat comes from a person within the organization. It can also help to mitigate the threat surrounding zero-day attacks. A zero-day refers to an exploit that has not been discovered by other security researchers yet, which is the most dangerous type of exploit to be discovered because it is generally difficult to detect. With UEBA, on the other hand, it is highly possible to detect abnormalities and act on threats before they have the chance to conduct too much damage to the organization's infrastructure. If inside threats are mentioned as a challenge in the framework by the organization, then CASB's UEBA abilities will be able to solve this. The second pillar is analytics which is tied to the use of machine learning and statistics in order to analyze all the data that is gathered. The third pillar is the data the UEBA system will analyze. In most cases, the types of data that a system needs is network traffic, as well as other events and logs that the SIEM solution produces. The UEBA tool implemented needs to combine forces with the organization's SIEM solution. This is because the SIEM solution can provide useful data to make the UEBA algorithm even more accurate.

A CASB solution can provide logs that contain user account activity in the cloud environment. This gives the organizations options to block unauthorized users and other malicious activities. User and Entity Behaviour According to Ahmad, Mehfuz, and Beg 2020 analytics provided by a CASB can monitor users, devices, and different application activity and detect abnormality these processes produce. In order to detect these abnormalities, CASB UEBA uses machine learning to profile each user in the cloud network.

CASB UEBA machine learning algorithm creates patterns of user activity based on their normal behavior. If a user is flagged for abnormal behavior, that can pose a potential threat to the organization's cloud network. Some CASB providers also utilize UEBA in order to create a scoring-based system that will give each application, device, and user account in the network a score. This score is then used to determine if a user account is allowed to perform certain actions, which can range from using an application to downloading a confidential document.

According to Rajat Wason 2020, CASB can also be deployed with UEBA as a standalone service. Gartner claims that CASB based embedded UEBA is really important since the user activity or interactions are not as visible to other services that offer UEBA as a standalone feature. meaning that the data collected from a CASB can provide a more accurate user profile for the UEBA machine learning algorithm.

Also, according to Khaliq, Abideen Tariq, and Masood 2020, CASB can be implemented with a machine learning-based CASB model. This implementation model is meant to increase the UEBA experience and make the machine learning algorithm more accurate. In the CASB terminal, the organization would be able to see the different profiles that the UEBA algorithm has created, and each entity in the network will have its own score. When something is wrong, the CASB solution will flag the event, and the organization would be able to see exactly what happened and which user account, and what service the event is about. These events have to be monitored by security professionals to take action each time something is flagged as abnormal and improve the algorithm. Over time, the machine learning algorithm will become more accurate by learning from itself, and the entity profiles will be more suited for the organization, potentially producing fewer false positives.

Varonis 2020 brings up both the positive and the negative aspects of using UEBA services. For one, it is great for automatically detecting unusual behavior in the network and reducing the time to detect multiple security threats. However, on the contrary, Varonis 2020 states that it can be costly, especially if it is a smaller size organization that wants to acquire these services, as well as not an outright replacement for other security measures.

Shadow-IT

Because of rapid cloud development, many organizations have been deploying business processes into a cloud environment. When a security or IT team in an organization does not have control over applications or processes in the cloud, Shadow-IT is called. This can be a variety of different things, but it is mainly referring to applications in the cloud that the organization does not know about.

Shadow IT is defined as any hardware, software, or services built, introduced, and used to work without explicit approval or even knowledge of the organization according to Mallmann, Maçada, and M. Oliveira 2018. The motivation is to complete work tasks by using other tools than the organization/company has provided. However, Shadow IT differentiates from similar concepts such as workarounds, BYOD, and IT consumerization by the objective of the user. With Shadow IT, the primary objective is to complete work tasks effectively and productive, but the company's provided tools hinder the effective completion. The hindrance can stem from either malfunction or inadequate organizational IT systems or instructions, implying that employee needs are not met. Cloud computing is a constantly progressing field of study, and new solutions are produced in a pace that the IT department of a company might not be able to follow. Therefore, it will be a gap in what a regular cloud computing consumer can use for private reasons and what tools a company adopts into their toolkit. It can be argued that it will always exist a gap because new IT solutions should be evaluated before they are implemented.

So why is this a problem? Shadow IT is a phenomenon that has gathered increasing attention proportional to how many services are offered as cloud-native solutions. In a survey from 2016, CIOs and IT managers were asked about Shadow IT, and of the 200 participants, 72 percent reported that they do not know how Shadow IT is being used within their organization as also stated by Mallmann, Maçada, and M. Oliveira 2018 implying that they do not have control on what users are doing. Shadow IT can be both positive and negative. The positive side is that it can spark innovation and be more beneficial for employees. The negative side, as presented by Sillic 2019 is that Shadow IT can undermine the official system, damage organizational processes and data, result in compliance issues, wasted time, inconsistent business logic, increased risks for data loss or leaks, and wasted investment.

Chapter 6

Reflection and Learning

The Reflection and Learning stage is a continuous stage that parallels the first two ADR stages of Problem Formulation and BIE. The parallelization is important as the learning that emerges from the ADR process is an important input to adjust and improve the artifact in future design cycles.

6.1 Emerged learning

6.1.1 Learned What CASB Can Do

By reviewing literature and documentation from different CASB vendors, the researchers could paint a picture of all the potential capabilities a CASB might consist of. From the research, it emerged that a single CASB could not deliver all of the features at once. Therefore a CASB should be viewed more like a toolkit than single software that has all the listed features. Furthermore, by learning all the possibilities of a CASB, it was also easier to see which technologies that compete against a CASB.

6.1.2 Requirements

As detailed in the Problem Formulation chapter, Sykehuspartner is in a position where they want a description to justify the decision if they should buy a CASB or not. A list of demands did not help to understand further what a CASB consists of and how they can utilize a CASB. The initial thought was to provide a list of requirements if there was discovered a need for CASB so that when a vendor contacted the provider, the list could be provided so that the CASB was tailor-made. A list of requirements proved to be a dead-end, as the problem was to justify a decision of whether a CASB is worth it or not. It is also complicated to follow such a list for a vendor, as the product is in a state of innovation, meaning it is constantly changing. Requirements will also quickly be outdated, as the organization's needs might change, and will also not provide any information on the applicability of a specific CASB.

6.1.3 Need-analysis

During the first draft, the framework was intended to be a need-analysis for Sykehuspartner, as further elaborated in the BIE chapter. However, this was created as a self-evaluation that did not help Sykehuspartner solve the initial problem. What we learned from bringing this to Sykehuspartner was that this was too little information in order to be able to help them decide.

The goal of the first version of the framework was to examine if Sykehuspartner needs a CASB, and the tool to evaluate this need was intended to be a need-analysis. The researchers learned that a need analysis is a complex field, but more importantly, the evaluation of need is not answering the problems of Sykehuspartner. One of the reasons need is a difficult measure is that an argument can almost always be made that new security technology is needed in information security. The more important question to ask is if the new technology improves the security to an extent where it makes sense to buy. In an evaluation process, the investigation of technological needs proves fruitless as technology is inherently in a state of constant improvement and innovation. Therefore, an evaluation needs an equal focus on aspects other than technology, such as financial and legal perspectives.

6.1.4 Trying To Save The World

When we created the first draft, it contained information on all the aspects of CASB. Based on the feedback from the practitioners, the framework had to be scoped, so it contained information regarding three features of CASB; UEBA, Shadow-IT, and Access Control. Initially, we included all the possible features of CASB, which proved to be impractical. By scoping these features, we could also provide more appropriate information and data on each subject, rather than trying to bring everything to the table at once.

The initial framework was to be based on all the technologies that can fit inside a CASB toolkit. However, it soon proved very difficult to encompass all the aspects when the list of technologies was very long. Also, it proved very tedious and time-consuming for participants to complete a survey, which again is negative in an organizational environment of security where time is of the essence. A long list of possible features did also not answer the problem of understanding CASB as a technology and how CASB possibly will fit into the existing environment. The list of possible features was also very time-consuming to find good documentation on, as some of the technologies were provided more as bonuses and not as core functionalities. Bonus features should not be compared at the same level as core functionalities because different vendors might not provide the same service.

6.1.5 Questions

The questions from the first draft were based on research and different types of vendors that offer CASB as a service. What we did learn there was a lack of knowledge of what CASB offered. Vendors said that CASB can be used for malware detection or as a firewall in the cloud, but is it a reason to buy a CASB if the organization already has solutions for this? We learned that it was hard to answer these questions based on the exciting research on CASB and each vendor's explanation.

Questions were designed to be based on literature, as the aim was to provide a view of how literature defines a CASB to evaluate if a CASB can fit into the existing environment. The questions proved difficult for a participant to answer, as they required a thorough understanding of every part of the existing IT environment.

The idea behind the questions for the second draft was to create questions that helped Sykehuspartner self-evaluate the situation. Nevertheless, the fact that the framework tried to answer the task of justification with questions proved difficult as Sykehuspartner initially had questions they could not easily answer themselves. Therefore, the framework ran into the problem of answering questions with more questions. Based on feedback from the previous draft of the framework, the questions were focused more on explaining what each of the different technologies could provide. The structure of explaining more helped understand what a CASB might provide, but the questions were too focused on a hypothetical situation of what might happen. Sykehuspartner needed more precise ideas of a CASB to evaluate if a CASB is better than the technologies they already utilize. One of the essential discoveries during this round of feedback was that the framework did too little to evaluate the situation Sykehuspartner is in at the time. The discovery was that a more comparative approach was needed. Therefore, the idea was to incorporate more things to make it possible to measure if the improvement is possible.

6.1.6 Scoring system

The second version of the framework also had a scoring system, as presented in the BIE chapter. What we also learned from the practitioners, in this case, was that scoring could be misleading. If the risk is based on a single integer score, then that score alone cannot justify a high or low risk. The explanation derived from the discussion in the ADR team was that risk has to take multiple aspects into account when calculated.

An inherent problem of using a scoring system is that values used to present the result might cover up essential nuances. The score of need, for instance, was hard to make understandable. If the framework presented the score of Sykehuspartner needing a CASB technology as an 8 out of 10, what does that eight mean? To make such a scoring system work, the scoring has to be based on a scoring system proven to accurately represent need. Such scoring systems must be created and proven for each of the capabilities of ROI, need-analysis, and risk.

6.1.7 Key Performance Indicators

The second draft had the return of investment as a score in combination with the risk. Using ROI was not helpful, as the return of cost depends on future predictions making it an unreliable form of measurement. During the discussion with Sykehuspartner, we learned that it was better to implement key performance indicators measuring the success of CASB instead of trying to carry out a score for ROI, which Sykehuspartner indicated as difficult for security tools. A key performance indicator was a feature they could later use to measure the effects CASB had on their cloud environment.

6.1.8 Challenges

Also, during the feedback from the second draft of the framework, we learned that it is more efficient if the organization fills out each challenge independently. If we presented this framework to another organization, each challenge would be different based on the security policies, cloud strategy, cloud architecture, security measures implemented, and size. This difference means that each organization should create its own set of challenges. Challenges feel very natural to use when considering the use of KPIs for measurement. As every challenge that an organization faces consists of at least one KPI to measure.
Example: An organization, O, views increasing the number of customers as a challenge. The challenge of customer increase can be measured by counting the number of customers and comparing it with the same count over time. Analysis of these numbers will provide insight into if an organization increases customers or not. However, the numbers will only provide an overview of the consequences and not any insight into why the numbers are behaving as they are.

6.1.9 Platform, not a toolkit

Another essential aspect that we learned during discussions with Microsoft was that CASB is often referred to as a platform rather than a security toolkit. Microsoft mentioned CASB as part of a package or platform with other security measures. This perspective means that CASB is not a measure that an organization buys on its own but instead in other security tools.
The MCAS will not defend against malware and attackers in the cloud alone, but together with, for instance, Microsoft's Endpoint Manager, it can function as a good defense measure for cloud security. An example of how the MCAS functions as a platform rather than a toolkit: By utilizing MCAS together with Defender for Endpoint, eventual attacks on a client will impact the client's level of access. A client registered in Endpoint Manager might be known to MCAS via Azure AD, and by that, get access to other things compared to the use of an unknown client.

6.1.10 Who watches the Watchmen?

As previously discussed in chapter 5, it is essential to understand the scope and value of any new security technology for an organization. Security technology with a large area of responsibility must be considered in operation and maintenance over a more extended period of time. It is not sufficient to only consider technological perspectives. Adopting a cloud security technology with capabilities that creates visibility and control over the cloud environment must also consider the people who operate the technology. A healthcare service provider must, for instance, consider the security clearance employees need to operate the technology. When acquiring a CASB, there should be a common understanding of precisely what it will bring to the organization. The CASB will handle a large amount of organizational data, and it is then significant to know how the CASB will handle these data. For example, a question that should emerge is: How does the CASB handle privacy related to all the data gathered for UEBA?

6.1.11 Categorization of Challenges

During the workshop, we presented the final draft to several cloud experts within Sykehuspartner. One of the reflections we did during this workshop was that each challenge should be categorized. This categorization is helpful because one person can generate challenges only based on his or her view. For example, say that person is very technical, then the list would be filled with only technical challenges. Categorizing the challenges and giving each color made it easier to see which categories the table of challenges lacked or which one was too frequent. The categorization is another step to increase the possibility of covering all the aspects an organization might face when utilizing cloud services.

6.1.12 The type of challenges

From the workshop, it emerged that standardization of challenges to be put into the framework is beneficial. The framework is only as good as the challenges that are put into it, and it will therefore benefit the organization if challenges are collected from sources such as CSA or OWASP to have the highest possibility of covering all the aspects that the organization is facing. To remove bias from the input of challenges, it is of great advantage that challenges are based on models like CSA's.

6.1.13 Filters

Another aspect the experts brought up was the possibility of adding more filters to the framework. If the organization wants the framework to cover every aspect or a specific aspect of CASB, they can add filters as they wish.

The filters proved to be a valuable method of checking every technology that a CASB can consist of. The value comes from the modularity, as the filters can be replaced and altered to fit exactly the type of CASB that Sykehuspartner is evaluating. As CASBs are modular, the framework modularity is an important feature. For each filter to work as intended, every participant must read the explaining text to ensure that everyone has the same understanding of what the technology consists of.

6.1.14 Weighting of Each Challenge

Since each challenge is brought through all filters in the final version of the framework, each challenge will greatly impact the result. One of the things we learned from the workshop was that each challenge should be weighted differently. For Sykehuspartner, one challenge may weigh more than ten others, which implies that it is important to score each one based on the organization's needs.

The intention of weighing the challenges after the challenges have gone through the framework is to create an organizationally specific view of what a CASB might provide of value. As the weighing is up to the organization, it forces the participants to choose how important different challenges are. The importance of each challenge will most likely be very colored by the background of the participants. If the participants have different backgrounds, the result of the discussions will therefore be more informed.

6.2 Reflection on the Literature

The literature is stating that there are many benefits to utilizing the cloud for a healthcare service provider. Benefits include easier sharing of data, together with an improvement in the spending of resources. Cloud computing will therefore be able to let healthcare service providers save both money and time. Reviewing the literature points towards clear advantages for healthcare service providers with adopting more cloud services. However, there are special risks that the infrastructure in a hospital faces due to the nature of the sensitive data and critical position in society. Denial of service is potentially very critical for a healthcare service provider. There is a notion of cloud also being a possible danger to healthcare service providers, but there are not developed many tools tailored to the need of a healthcare cloud. Reflecting on the literature gives little insight to what healthcare organizations can do specifically to better their cause. Therefore, the next best approach is to treat healthcare service providers as a large generalized organization. Because there are more tools and literature relevant for enterprise, including organizations, in general.

For securing cloud services, it has emerged several technologies that seek to answer these sorts of security problems. According to Gartner, one of the most promising cloud security solutions is a CASB. A CASB solution will work as an intermediary between a CSP and a CSC, specializing in security measures. Important features advertised for a CASB are Shadow-IT discovery, Access Control, and UEBA. Together with these controls, technologies such as DLP are also advertised as great promising features of a CASB. However, in the Shackleford 2021 CASB is presented as a part of a SECaaS product. Reflecting on the research and advertisements, the researchers believe that CASB is one of the most praised cloud security technologies in the cloud security market. Gartner estimated in 2015 that 85% of organizations would use a CASB within 2020. This prediction has turned out not to come true. The SANS survey from 2021 Shackleford 2021 suggests that there are almost no changes from 2019, and the number stays at under 60%.

The review of literature also uncovers that a CASB is discussed positively, without a thorough description of how CASB is implemented. Different deployment modes are discussed without mentioning important details. Obregon 2017 discusses different deployment modes, without mentioning that most CASB requires existing technology such as firewalls (e.g. Bitglass Inc. n.d.) or specific operating systems (e.g. Microsoft n.d.(a)).

Adopting a new cloud security technology is a complicated process, and important factors have been shown to include Relative Advantage, Complexity, Technological Readiness, Top Management Support, and Firm Size. The importance of adopting new cloud security technology for a large healthcare service provider is of great significance, as the paradigm of cloud computing promises great rewards. However, great dangers are also related to the adoption of cloud technology. Therefore, it is very important that the decision-making process is as good as possible to ensure that the technology will positively impact the organization over a sustained period of time. The decision-making process is however very complex, and the literature indicates that not only does it exist a need for better decision making in information security but the decision-making process in healthcare organizations as well is also in need of improvement.

The literature indicates that the decision-making process for IT security officials in a healthcare service provider is complicated. The case of cloud security service adoption emphasizing how complex a decision can be. There is a great incentive for healthcare services to implement cloud services due to reduced cost and increased efficiency for medical professionals. Even though a cloud security technology is beneficial, it must be justified to all the stakeholders, a large healthcare organization with many different perspectives, which means that a cloud security expert focusing only on the technology will not be able to justify its adoption. There is a need to consider different aspects, such as business drivers and the organization's risk with the new technology. A term such as risk is very complicated to discuss with different stakeholders due to different understandings of what risk to the organization means.

With the existing research in mind, this paper contributes to enlighten the acquirement of an intermediary between the cloud service provider and a healthcare organization's cloud environment. As mentioned by Thomas Vandermarliere 2016, there is still a need for more research on CASB and how it fits into an enterprise cloud network. On the other hand, according to Tervoort et al. 2020b the healthcare sector is seeing an increased amount of cyberattacks. In addition, the authors mention that medical records can be sold for more than ten times that of credit cards on the black market. Mandal, Sarkar, and Chaki 2014 also explains that there is a more prominent need for a cloud strategy when pushing to a cloud solution within a healthcare organization.

Another essential aspect that learned during this project is the fact that CASB might not be the perfect solution that Gartner claims it is. According to Gartner n.d.(b) CASB can help the organization with security policies, authentication, encryption, malware detection. Through our thesis, we have learned that CASB cannot solve these problems on its own. CASB has to be implemented in combination with traditional on-premises IT infrastructure. CASB can then be a helpful tool to make security in the cloud more sturdy; it will not function as a security product on its own. The CASB is built as a security add-on. That means that if the organization is not mature enough, then acquiring a CASB might not be the right choice for them.

Utilizing an intermediary in order to secure the enterprise cloud environment appears to be a less researched area, at least to the best of the authors of this paper's knowledge.

However, research towards cloud security is broad and contains multiple valuable sources that provide well-written research on this topic. Mukherjee 2019 states that cloud computing unlocks a new world of possibilities and advantages while also mentioning that the security aspect of migrating a business to a cloud environment can be dangerous. Many organizations migrate their business processes to cloud computing in order to gain more effective solutions, which then opens up for more security challenges according to Shuaib et al. 2019.

Chapter 7

Formalization of Learning

As detailed in the previous chapters, the ADR process of this project has resulted in a Decision Support Framework prototype that represents the larger class of problems regarding decision support for security officials in a public healthcare service provider. This chapter will discuss the contributions of the framework and the contributions of the learning that have emerged during the ADR process.

7.1 Can the learning answer the general class of problems

As defined in chapter 4, the class of problems is formulated as *Decisions for security officials in a public healthcare service provider.* The result of the ADR process is an artifact that can help an organization get a better understanding of a CASB and if a CASB can improve the cloud environment or not. It turns out that the framework is very flexible, and it emerged during the workshop with security professionals that the framework can be equally as valuable for another setting. Because the filters in the framework does not need to be restricted to a CASB. The descriptions of each technology are useful to let participants get a common understanding of the technology that is described, regardless of the setting. The challenges will also be customizable; although the challenges an organization or company face will likely be the same regardless of the technology, it is still possible to test each of the challenges against the technology described in the filter. If the organization's challenges are the same, it will be possible to use the framework to compare the impact of different technologies considered for adoption. By evaluating which of the applicable technologies that solves not only the largest amount of challenges an organization face, but also evaluating which technology that solves the larges amount of important challenges, the quality of the decision process will be improved. The decision-makers in the organization can feel more confident that the technology that is adopted is the best option. Therefore, the framework will most likely improve the decision process regardless of the technology that it represents, which is why the framework answers to the larger class of problems. This result indicates that the framework is generalizable and that the contribution is relevant for other problems than discussed in this project.

7.2 Design Principles

During the design of the artifact, several topics emerged as important considerations. The topics are detailed in chapter 6. These considerations will be applicable for any other design process that seeks to create a framework or tool to help security officials in a large healthcare organization ensure quality in their decision making process. The considerations are generalized in the ADR process as Design Principles, and the Design Principles that emerged during the artifact design consists of:

7.3 Limitations of the framework

As the project is a master thesis, there have been certain limitations in the project work due to the nature of the project work. The project has also been a learning experience for the researchers, meaning that some of the work has been planned and altered as the project progressed.

7.3.1 One Organization and Sector

One of the important limitations to the presented framework in this thesis is that it is only tied to one organization and one sector. In order to scope this thesis, the focus was set on healthcare and CASB, respectively. This thesis is limited to only the aspect of security in the cloud from a healthcare perspective, which again is tied to a Norwegian healthcare organization.

7.3.2 Time

As stated by Sein et al. 2011, one of the most critical elements is to develop a long-term commitment from the organization that you are collaborating with. This means that the BIE cycles will become more accurate if the researchers are given more time. This thesis is limited to only conducting meetings with Sykehuspartner for three months, which still gives time for a finished artifact; however, the artifact could always use more feedback. In addition to this, the perspective of time related to the workshop was too small, meaning we would have wished to conduct multiple workshops during a longer time period. However, due to tight schedules for the employees of Sykehuspartner and restricted time for the researchers, this was not possible to execute.

7.3.3 Self sufficiency

The framework cannot answer any questions definitively on its own; it needs more information from other sources. It is therefore not a self-sufficient framework. To give a clear answer for decision-makers, other tools are also needed in the process.

Design Principles	**Description**	**Evidence**
KPI to measure improvement	It is better to use KPI to compare the impact of a security technology, than using ROI as a measurement.	ROI is not feasible to use as a measure of how good a cybersecurity technology is
Do not use scoring	A scoring system is not productive to use in an analysis measuring the need for a new cloud security system. The quantification of abstract values is first and foremost difficult, but it is also very hard to understand for the person trying to read information out of the scoring system.	Information is lost in the process of quantifying complex information
Describe rather than question	Description of technology will improve the understanding	It is hard to answer questions with more questions
Need analysis is redundant when evaluating security technology	It is better to assess the impact a new technology might have on an organization's challenges, rather than trying to analyze what their need is.	The need for new security technology can always be argued to exist. Security is never 100% covered.
CASB should be referred to as a platform	CASB is more a platform than a single technology that fixes all on its own.	Microsoft sells their CASB as part of a platform.

Table 7.1: Table containing the different Design Principles derived from the artifact

7.3.4 Bias

Sampling Bias

One bias that could impact the result of this paper is the limitation towards only sampling data from one organization within one sector. The given result can be biased since it is solely based on the gathered data that we were provided from Sykehuspartner. In other words, the result might only apply to Sykehuspartner and not other organizations, which might get a different outcome suggesting that a decision framework does not help evaluate a security technology.

It is important to note that a small portion of the papers we use in the literature review are based in other countries which have different infrastructures compared to Norway. An example is the Ouardi, Sekkaki, and Mammass 2017 which context is based on data from Morocco that has an entirely different perspective compared to Norwegian healthcare organizations. In other words, this difference in the environment will bias the result of the literature, and the results discussed in the literature may not be applicable in our scenario. If Norwegian healthcare has a more digitized infrastructure compared to Morocco, it will mean that Norway might be relying more on cybersecurity solutions.

Confirmation Bias

The ADR process is a qualitative form of research, and inherent in qualitative research is the risk of confirmation bias. We might be tempted to find a solution to our problem, and this motivation can result in confirmation bias. The impulse towards highlighting which evidence that was used to argue for our result can often create a confirmation bias and end up rejecting a review or measurement that might have altered the result according to Edgar and Manz 2017. In other words we might have forgotten, for example, to discuss data that we got from the workshop or ideas that were brought up in one of the meetings during the BIE cycles.

Ambiguity Bias

Both due to the problem being a wicked problem, and our focus on existing technology in CASB, might result in an ambiguity bias. The bias occurs when we are faced with great uncertainty and might bias us towards over-focusing on known knowns rather than exploring new possibilities.

7.4 Theoretical Implications

7.4.1 CASB to CASP

We argue that there is a need to shift the focus away from the technology as a broker and focus more on the applicability of the technology as a platform for different security services. However, there must be a clear distinction with the existing term of Cloud Application Security Platform, as the latter term is focusing on cloud-native applications and on their APIs. There is a need to still focus on the access control aspects of a CASB, but with the inclusion of the term platform. The Cloud Access Security Platform term will serve as a notion to connect different methods of access control through the platform.

7.4.2 A Need for More Practical Studies

The project work has highlighted the need for more research on how a CASB fits in an organization. There is a need for case studies of organizations implementing CASB. There is also a need to evaluate the efficiency of a CASB in a multi-cloud environment, together with the need to research alternatives for multi-cloud environments. Research is also needed to evaluate how a CASB fits into a SIEM.

7.4.3 A Focus on Improvement of Existing Infrastructure

Our work suggests that there is a need to clarify how a CASB can improve on existing security technologies, further indicating that there is a lot of research needed to prove that a CASB is worth adopting for large healthcare organizations. CASB alone cannot solve the challenges associated with cloud computing. However, CASB should be viewed as an addition to other security features that the organization already has implemented.

7.4.4 Similarities with Unified Threat Management

Unified Threat Management (UTM) puts different security solutions together to create an all-in-one security solution. This is a type of security solution that was intended for SMBs, as it offers an affordable security solution that covers some important parts of the business. The structure of CASB is very similar to UTM; one can even argue that they are the same thing. The difference is that UTM is a mindset that became popular in the early 2000s, whereas CASB is a technology that has arisen from the need to identify Shadow IT some ten years later. The similarity is that both offer a "kit" of security solutions. One can argue that a CASB is better suited for an SMB than a large organization because of these similarities.

7.4.5 Extend the TOE framework

We argue that security decision-makers in healthcare should take into consideration challenges categorized from not only the TOE framework but extend it with the categories of Economics and Privacy. Liu, Chan, and Ran 2016 proposes a combination of cost and TOE in their study, and we suggest that the use of the TOE framework to evaluate different challenges an organization faces also takes into consideration privacy, third party factors, and a cultural/human aspect.

7.4.6 Numbers hide information

Based on the Design Principle "Do not use scoring", we argue that decision support systems utilizing numbers are not sufficient to support decisions in cloud security for a healthcare setting. Due to the nature of a wicked problem (Pries-Heje and Baskerville 2008), which decision making in this setting falls under, information in these problems are very complicated. Numbers swallow up too much information, and information is also lost in the process of interpreting what the numbers represent. We argue that this finding is a result of a practical approach to problem-solving.

7.5 Practical Implications

The research of this project has detailed the difficulty for IT security to make decisions on the adoption of cloud security technology due to the complexity. Also discovered is the importance of understanding the technology that is to potentially be adopted. Our work has created a framework that helps decision-makers understand the technology better while also assessing the impact the technology might have on the organization. This information will help the decision-maker argue that the decision is the best decision for the organization. By utilizing a framework, it will be possible to show the thought process behind the decision so that it will be easier for people outside of the process to understand what basis the decision is made on. The framework will therefore let decision-makers be more certain that the decision is beneficial.

Utilizing the framework with CASB as the technology in question results from the workshop with security professionals from Sykehuspartner implied that a CASB would benefit the organization. However, feedback stated the need for more information to make a decision. The lack of information is due to limitations of the framework but also due to information on CASB being very scarce from vendors on how a CASB will improve existing infrastructure. The result is also very colored by sampling bias, as the sample size of challenges was minimal and not completely covering all the problem areas that Sykehuspartner must consider when utilizing cloud security controls. The result of the workshop is also not taking into consideration how well a CASB is performing compared to existing technologies or compared to other cloud security technologies on the market. Because of the lacking information on how a CASB can improve on existing security measures, it is as of now very hard to justify the procurement of a CASB.

Also, what emerged during the stage of research is that all the specific tools and technologies that CASB might possibly provide are not likely to be better than the same services provided by vendors that specialize in similar services. An example is that a company that delivers a service that is completely focused on DLP is more likely to be useful to the organization than a DLP service provided as part of a larger CASB toolkit. However, buying different services from different vendors also extends the list of possible vulnerabilities and the list of vendors that the organization has to rely on. Buying different services from different vendors will also possibly increase the friction that a user experiences, together with the fact that paying small vendors for exclusive services is likely to be more expensive than the payment for a single service where every tool is provided.

CASB is not a cloud security measure that can be implemented on its own, it needs an existing infrastructure to function.

7.5.1 Design Thinking

The workshop seemed to be able to draw similarities to the design thinking methodology. This methodology is a way of interacting with certain new technologies in order to make the end-users or the decision-makers to be able to understand it better. Design thinking is meant to help the organization in order to create a more accurate vision of the new technology. According to Dym et al. 2005, design problems are structured in a way that the designer has a customer who has a set of users that will benefit from a designed artifact for the given problem. As Dym et al. 2005 further elaborates, one of the characteristics of a good design is the ability to make decisions, being part of a team, and handle uncertainty. In addition, Dym et al. 2005 mentions that one of the ways design thinking can be utilized is by conducting collaborations with practitioners, researchers, and experts. Design thinking is, in other words, method in order to improve learning and reflection of designing engineering products. In this particular case, the workshop functioned as one of these collaborations with those who build the design, as well as the end-users who will utilize the result. In that case, it was easier to understand the design and the approach made by the researchers.

7.6 Strength of contribution

Our contribution is a practically oriented approach to researching cloud security controls, with a special focus on CASB technology. The result of the practical research is a framework that helps security decision-makers in a healthcare service provider in their decision-making process as they work with decisions on wicked problems.

As of now, the artifact presented in this thesis can benefit large healthcare organizations in deciding on cloud security solutions. Specifically, the framework is tailor-made for Sykehuspartner since the design was established in collaboration with them and based on their feedback. That does not mean that the healthcare sector is the only type of organizations that can benefit from a decision-based framework, and it can be applicable to other organizations within different sectors as well.

State of the art regarding the current understanding of cloud security control adoption is that the understanding in literature is limited for security decision-makers in a large healthcare organization. The nature of decisions a security official in a large healthcare organization works with are in their nature wicked problems. Knowledge of wicked problems in connection with cloud security control selection and a large healthcare organization is lacking. There is also limited understanding of how a CASB can impact a large healthcare service provider.

The framework is relevant as the adoption of cloud solutions continues to increase, with Covid-19 as a major motivator. In addition, cloud computing is becoming more and more popular in order to create more effective and cost-reducing solutions for organizations. More data is being processed in the cloud, as well as new applications are developed in rapid succession, and organizations that adapt to the cloud business model have to stay up to date on the technology in order to secure their infrastructure from threats. There are multiple cloud security controls in development, and in that regard, the proposed framework in this paper can be relevant in the decision process for cloud security solutions.

Findings from the project are rigorous due to the ADR process ensuring a strong practical influence as practitioners from the field of information security were an important part of the design process, which means that the framework was made to apply to a real-life scenario.

7.7 Future Work

Due to limitations such as time and knowledge, the researchers are very clear that more research and testing are needed before any of the results can be used in practice. There is also a need to verify the findings that have emerged during the project.

7.7.1 Design Thinking

As previously mentioned, the Design Thinking methodology introduces more case studies, workshops, and other forms of interactions between professionals to better understand new technology. One aspect that can be further developed in future work is the experiments on how design thinking can improve decision-making within an organization. By conducting more workshops similar to the one performed in this thesis, the design thinking methodology can be a new way of introducing new technology, not only limited to security. Furthermore, design thinking is highly related to engineering and creating discussions and interactions between different employees, which can be further researched with a similar artifact from this thesis.

7.7.2 Expansion of Organization and Sector

As mentioned, one of the limitations of this paper is the research towards only one organization and one sector. This could be further expanded in future work, where the researchers could choose to look into another aspect. Rather than healthcare, researchers can, for example, look into applying the same context to a university. In addition, this research has a functioning artifact for CASB, which can be further elaborated by involving other tools as well. Say an organization wants to implement an on-premise security solution, then the filters in the presented artifact could be switched out to suit the new on-premise solution instead.

7.7.3 Wicked Problems

Decision-makers in a large healthcare organization face wicked problems in other areas than the decision on cloud security controls. It will therefore be an advantage to better understand the nature of wicked problems in this setting. Further research to address how security decision-makers in a healthcare organization can answer wicked problems is needed.

7.7.4 Other scenarios

The framework shows signs of applicability for other technologies than cloud security technologies in a healthcare service provider. However, how well the framework performs in other scenarios with a technology of different nature must be validated.

7.7.5 Possible Future Research Areas

- The limitations of CASB
- CASB must be compared with other technologies to evaluate the performance
  - Will a CASB be able to perform better than ordinary logging systems for the cloud?
  - Will a CASB be able to outperform a Secure Encryption Gateway?

  - CASB in comparison to Splunk?
- Total Cost of Ownership comparison with other technologies
- Difference between CASB vendors - Which CASB vendor provides what services

Chapter 8

Conclusions

The body of literature in this report indicates that healthcare service providers will benefit from cloud solutions due to functionality such as reduced cost and improved efficiency of healthcare information exchange. At the same time, security controls must be in place before healthcare organizations can utilize the cloud. However, the selection of cloud security controls is a wicked problem by nature. Our work has therefore consisted of working towards a solution for the wicked problem. The method used to create an artifact to answer the wicked problem is ADR. The artifact design was developed during the building, intervention, and evaluation cycles in the ADR methodology. Choices on intervention of the framework were discussed inside the ADR team, and changes on the framework were chosen to suit the organization the best way possible. The result from this thesis is a framework that can help decision-makers evaluate the impact of cloud security controls. The framework will let participants in the decision-making process see how the different aspects of CASB can impact challenges that the organization faces, and compare the impacted challenges to highlight how significant the impact is. If the decision-makers are able to understand and evaluate the security control, then it is easier to make a decision in which this framework can guide organizations in the right direction. As of now, the framework is tailor-made for the healthcare sector based around CASB as the security control. Even if the end-users of the framework have different visions and opinions on the evaluated security control, the resulting artifact can still create valuable discussions on the subject. Our proposed framework also addresses a gap in the literature regarding the lack of definition of CASB and design science research papers.

The most significant findings from our project can be summarized to:

- Common understanding is beneficial
- Discussion will help create a common understanding
- Design principles that can be used to create decision support frameworks for security control selection
- It is a more precise practical approach to consider CASB as a platform
- There is a need for more practically oriented studies that focus on the application of CASB
- More studies that compare CASB to existing technologies like UTM
- Understanding of wicked problems that a security decision-maker encounters in a healthcare service provider is necessary to create relevant decision support tools

Our findings fit into the view that a selection of cloud security control in a healthcare service provider is an ill-structured or “wicked” problem that requires a unique problem-solving approach.

Bibliography

(CSA), Cloud Security Alliance (July 2015). *Gartner's Latest CASB Report: How to Evaluate Vendors.* URL: https://cloudsecurityalliance.org/blog/2015/12/07/gartners-latest-casb-report-how-to-evaluate-vendors/. (accessed: 28.05.2021).

Ahmad, Shahnawaz, Shabana Mehfuz, and Javed Beg (2020). "Securely Work from Home with CASB Policies under COVID-19 Pandemic: A Short Review." In: pp. 109–114. DOI: 10.1109/SMART50582.2020.9337121.

Al Mudawi, Naif, Natalia Beloff, and Martin White (2019). "Cloud Computing in Government Organizations-Towards a New Comprehensive Model." In: *2019 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 1473–1479. DOI: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00266.

Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos (2015). "Security in cloud computing: Opportunities and challenges." In: *Information Sciences* 305, pp. 357–383. ISSN: 0020-0255. DOI: https://doi.org/10.1016/j.ins.2015.01.025. URL: https://www.sciencedirect.com/science/article/pii/S0020025515000638.

Alliance, Cloud Security (2020). *Top Threats to Cloud Computing The Egregious 11.* URL: https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/. (accessed: 31.05.2021).

Atlam, Hany F. et al. (2020). "Risk-Based Access Control Model: A Systematic Literature Review." In: *Future Internet* 12.6. ISSN: 1999-5903. DOI: 10.3390/fi12060103. URL: https://www.mdpi.com/1999-5903/12/6/103.

Baron, Hillary et al. (2021). *State of Cloud Security Concerns, Challenges, and Incidents.* URL: https://cloudsecurityalliance.org/artifacts/state-of-cloud-security-concerns-challenges-and-incidents/. (Accessed: 01.06.2021.

Buchanan, Richard (1992). "Wicked Problems in Design Thinking." In: *Design Issues* 8.2, pp. 5–21. ISSN: 07479360, 15314790. URL: http://www.jstor.org/stable/1511637.

Chandrasekaran, Srimathi, Subaji Mohan, and Rajesh Natarajan (2015). “Survey on HealthCloud characteristics.” In: *Health and Technology* 5. DOI: https://doi.org/10.1007/s12553-015-0106-2.

Chang, Henry H., Paul B. Chou, and Sreeram Ramakrishnan (2009). “An Ecosystem Approach for Healthcare Services Cloud.” In: *2009 IEEE International Conference on e-Business Engineering*, pp. 608–612. DOI: 10.1109/ICEBE.2009.98.

Chauhan, Roma and Amit Kumar (2013). “Cloud computing for improved healthcare: Techniques, potential and challenges.” In: *2013 E-Health and Bioengineering Conference (EHB)*, pp. 1–4. DOI: 10.1109/EHB.2013.6707234.

CipherCloud (2020). *How do I automatically detect and remediate malicious user activity in the cloud?* URL: https://www.ciphercloud.com/user-and-entity-behavior-analytics/. (accessed: 11.03.2021).

Columbus, Louis (Oct. 2020). *What’s New In Gartner’s Hype Cycle For Cloud Security, 2020.* URL: https://www.forbes.com/sites/louiscolumbus/2020/10/25/whats-new-in-gartners-hype-cycle-for-cloud-security-2020/#:~:text=The%5C%20Gartner%5C%204Q19%5C%20security%5C%20spend,all%5C%20other%5C%20information%5C%20security%5C%20markets.. (accessed: 28.05.2021).

Coppolino, Luigi et al. (2017). “Cloud security: Emerging threats and current solutions.” In: *Computers & Electrical Engineering* 59, pp. 126–140. ISSN: 0045-7906. DOI: https://doi.org/10.1016/j.compeleceng.2016.03.004. URL: https://www.sciencedirect.com/science/article/pii/S0045790616300544.

Crowley, K. and B.W. Head (2017). “The enduring challenge of ‘wicked problems’: revisiting Rittel and Webber.” In: *Policy Sci* 50, pp. 539–547. DOI: https://doi.org/10.1007/s11077-017-9302-4.

Dang, L. Minh et al. (2019). “A Survey on Internet of Things and Cloud Computing for Healthcare.” In: *Electronics* 8.7. ISSN: 2079-9292. DOI: 10.3390/electronics8070768. URL: https://www.mdpi.com/2079-9292/8/7/768.

Dotson, Chris (2019). *Practical Cloud Security - A Guide for Secure Design and Deployment.* O’Reilly Media Inc. ISBN: 978-1-492-03751-4.

Dym, Clive L. et al. (2005). “Engineering Design Thinking, Teaching, and Learning.” In: *Journal of Engineering Education* 94.1, pp. 103–120. DOI: https://doi.org/10.1002/j.2168-9830.2005.tb00832.x. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/j.2168-9830.2005.tb00832.x. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/j.2168-9830.2005.tb00832.x.

Edgar, Thomas W. and David O. Manz (2017). *Research Methods for Cyber Security.* Todd Green. ISBN: 978-0-12-805349-2.

Elhabbash, Abdessalam et al. (2019). "Cloud Brokerage: A Systematic Survey." In: *ACM Computing Surveys* 51. DOI: 10.1145/3274657.

Fabian, Benjamin, Tatiana Ermakova, and Philipp Junghanns (2015). "Collaborative and secure sharing of healthcare data in multi-clouds." In: *Information Systems* 48, pp. 132–150. ISSN: 0306-4379. DOI: https://doi.org/10.1016/j.is.2014.05.004. URL: https://www.sciencedirect.com/science/article/pii/S030643791400088X.

Fortinet (n.d.). *What is Unified Threat Management (UTM)?* URL: https://www.fortinet.com/resources/cyberglossary/unified-threat-management. (accessed: 03.06.2021).

Gartner (2020). *Market guide for User and Entity Behavious Analytics.* URL: https://www.cbronline.com/wp-content/uploads/dlm_uploads/2018/07/gartner-market-guide-for-ueba-2018-analyst-report.pdf. (accessed: 13.04.2021).

— (n.d.[a]). *Cloud Access Security Brokers (CASB) Reviews and Ratings.* URL: https://www.gartner.com/reviews/market/cloud-access-security-brokers. (accessed: 28.05.2021).

— (n.d.[b]). *Definition of Cloud Access Security Brokers (CASBs) - IT Glossary | Gartner.* URL: https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs. (accessed: 24.05.2021).

— (n.d.[c]). *Gartner Glossary: Next-generation Firewalls (NGFWs).* URL: https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws. (accessed: 03.06.2021).

— (n.d.[d]). *Gartner Magic Quadrant for Unified Threat Management.* URL: https://www.gartner.com/en/documents/1941314-magic-quadrant-for-unified-threat-management. (accessed: 03.06.2021).

Georgiou, Dimitra and Costas Lambrinoudakis (2020). "Security and Privacy Issues for Intelligent Cloud-Based Health Systems." In: *Advanced Computational Intelligence in Healthcare-7: Biomedical Informatics.* Ed. by Ilias Maglogiannis, Sheryl Brahnam, and Lakhmi C. Jain. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 139–161. ISBN: 978-3-662-61114-2. DOI: 10.1007/978-3-662-61114-2_9. URL: https://doi.org/10.1007/978-3-662-61114-2_9.

Goel, Arpit (n.d.). *Is DLP a feature of your CASB or is it a pillar by itself?* URL: https://www.linkedin.com/pulse/dlp-feature-your-casb-pillar-itself-arpit-goel?articleId=6662011729792376832. (accessed: 30.05.2021).

Griebel, Lena et al. (2015). "A scoping review of cloud computing in healthcare." In: *BMC Medical Informatics and Decision Making* 15. DOI: https://doi.org/10.1186/s12911-015-0145-7.

Gutierrez, Anabel, Elias Boukrami, and Ranald Lumsden (2015). "Technological, organizational and environmental factors influencing managers' decision to adopt cloud computing in the UK." In: *Journal of Enterprise Information Management* 25.6. ISSN: 1741-0398. DOI: https:

//doi.org/10.1108/JEIM-01-2015-0001. URL: https://www.emerald.com/insight/content/doi/10.1108/JEIM-01-2015-0001/full/html.

Han, Peiyi et al. (2020). "CloudDLP: Transparent and Scalable Data Sanitization for Browser-Based Cloud Storage." In: *IEEE Access* 8, pp. 68449–68459. DOI: 10.1109/ACCESS.2020.2985870.

Hevner, Alan R. et al. (2004). "Design Science in Information Systems Research." In: *MIS Quarterly* 28.1, pp. 75–105.

Hong, Jin B. et al. (2019). "Systematic identification of threats in the cloud: A survey." In: *Computer Networks* 150, pp. 46–69. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2018.12.009. URL: https://www.sciencedirect.com/science/article/pii/S1389128618308259.

Hurst, William et al. (2020). "Patient Privacy Violation Detection in Healthcare Critical Infrastructures: An Investigation Using Density-Based Benchmarking." In: *Future Internet* 12.6. ISSN: 1999-5903. DOI: 10.3390/fi12060100. URL: https://www.mdpi.com/1999-5903/12/6/100.

Hussain, Nazmul (Dec. 2014). "Semantic Enabled Social-Collaborative Research Framework for Proteomics Domain." In:

Inc., Bitglass (n.d.). *What is a Cloud Access Security Broker (CASB)*. URL: https://www.bitglass.com/casb-cloud-access-security-broker. (accessed: 28.05.2021).

Inc., Broadcom (n.d.). *CloudSOC CASB*. URL: https://www.broadcom.com/products/cyber-security/information-protection/cloud-application-security-cloudsoc. (accessed: 28.05.2021).

Inc., CISCO Systems (n.d.). *Cloud Access Security Broker (CASB)*. URL: https://umbrella.cisco.com/products/cloud-access-security-broker-casb. (accessed: 28.05.2021).

Jackubczyk, Michal and Bogumil Kaminiski (2017). "Fuzzy approach to decision analysis with multiple criteria and uncertainty in healht technology assessment." In: *Annals of Operations Research* 251, pp. 301–324. DOI: https://doi.org/10.1007/s10479-015-1910-9.

Johnson, Robert and Chuck Easttom (2020). *Security Policies and Implementation Issues*. Information Systems Security & Assurance. Jones & Bartlett Learning. ISBN: 9781284199840.

Kaur, Shabnam and Rajandra Gupta (Oct. 2019). "Enhancing Features of Cloud Computing Using Cloud Access Security Brokers to Avoid Data Breaches." In: *European Journal of Engineering and Technology Research* 4.10, pp. 185–189. DOI: 10.24018/ejers.2019.4.10.1518. URL: https://www.ejers.org/index.php/ejers/article/view/1518.

Khaliq, Salman, Zain Ul Abideen Tariq, and Ammar Masood (2020). "Role of User and Entity Behavior Analytics in Detecting Insider Attacks." In: pp. 1–6. DOI: 10.1109/ICCWS48432.2020.9292394.

Kissoon, Tara (2020). “Optimum spending on cybersecurity measures.” In: *Transforming Government: People, Process and Policy* 14.3, pp. 417–431. DOI: https://doi.org/10.1108/TG-11-2019-0112.

Kreuter, Marshall W. et al. (2004). “Understanding Wicked Problems: A Key to Advancing Environmental Health Promotion.” In: *Health Education & Behavior* 31.4. PMID: 15296628, pp. 441–454. DOI: 10.1177/1090198104265597. eprint: https://doi.org/10.1177/1090198104265597. URL: https://doi.org/10.1177/1090198104265597.

Liu, Sen, Felix T.S. Chan, and Wenxue Ran (2016). “Decision making for the selection of cloud vendor: An improved approach under group decision-making with integrated weights and objective/subjective attributes.” In: *Expert Systems with Applications* 55, pp. 37–47. ISSN: 0957-4174. DOI: https://doi.org/10.1016/j.eswa.2016.01.059. URL: https://www.sciencedirect.com/science/article/pii/S0957417416300239.

Mallmann, Gabriela L, Antonio Carlos Gastaud Maçada, and Mírian Oliveira (2018). “The influence of shadow IT usage on knowledge sharing: An exploratory study with IT users.” In: *Business Information Review* 35.1, pp. 17–28. DOI: 10.1177/0266382118760143. eprint: https://doi.org/10.1177/0266382118760143. URL: https://doi.org/10.1177/0266382118760143.

Mandal, Amit Kr, Anirban Sarkar, and Nabendu Chaki (2014). “Flexible Cloud Architecture for Healthcare Applications.” In: *Applied Computation and Security Systems. Advances in Intelligent Systems and Computing* 304, pp. 103–121. DOI: https://doi.org/10.1007/978-81-322-1985-9_8.

McAfee (n.d.[a]). *How a CASB Integrates with an On-Premises DLP Solution.* URL: https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on-premises-dlp-solution/. (accessed: 30.05.2021).

— (n.d.[b]). *MVISION Cloud.* URL: https://www.mcafee.com/enterprise/en-us/products/mvision-cloud.html. (accessed: 25.02.2021).

Microsoft (2020). *Identify advanced threats with User and Entity Behavior Analytics (UEBA) in Azure Sentinel.* URL: https://docs.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics. (accessed: 09.03.2021).

— (n.d.[a]). *Microsoft Cloud App Security documentation.* URL: https://docs.microsoft.com/en-us/cloud-app-security/. (accessed: 25.02.2021).

— (n.d.[b]). *Top 20 use cases for CASBs.* URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3nibJ. (accessed: 15.02.2021).

Moore, Susan (n.d.). *Top Actions From Gartner Hype Cycle for Cloud Security, 2020.* URL: https://www.gartner.com/smarterwithgartner/top-actions-from-gartner-hype-cycle-for-cloud-security-2020/. (accessed: 28.05.2021).

Mukherjee, Sourav (2019). “Cloud-based Security Solutions.” In: p. 12. DOI: https://dx.doi.org/10.2139/ssrn.3408882.

Nair, Srijith K. et al. (2011). “Towards Secure Cloud Bursting, Brokerage and Aggregation.” In: *2010 Eighth IEEE Conference on Web Services*. DOI: 10.1109/ECOWS.2010.33.

Netskope (n.d.). *Market-Leading CASB*. URL: https://www.netskope.com/products/casb. (accessed: 28.05.2021).

Obregon, Luciana (2017). “A Technical Approach at Securing SaaS using Cloud Access Security Brokers.” In: *the SANS Institute Reading Room*. URL: https://www.sans.org/reading-room/whitepapers/cloud/technical-approach-securing-saas-cloud-access-security-brokers-37960.

Oliveira, Tiago, Manoj Thomas, and Mariana Espadanal (2014). “Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors.” In: *Information & Management* 51.5, pp. 497–510. ISSN: 0378-7206. DOI: https://doi.org/10.1016/j.im.2014.03.006. URL: https://www.sciencedirect.com/science/article/pii/S0378720614000391.

Ouardi, Abdesselam, Abderrahim Sekkaki, and Driss Mammass (2017). “Towards an inter-Cloud architecture in healthcare system.” In: *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6. DOI: 10.1109/ISNCC.2017.8071986.

Paul, Mridul and Ajanta Das (2018). “Provisioning of Healthcare Service in Cloud.” In: *Information and Communication Technology*. Ed. by Durgesh Kumar Mishra, Ahmad Taher Azar, and Amit Joshi. Singapore: Springer Singapore, pp. 259–268. ISBN: 978-981-10-5508-9.

Peng, Gang, Debabrata Dey, and Atanu Lahiri (2014). “Healthcare IT Adoption: An Analysis of Knowledge Transfer in Socioeconomic Networks.” In: *Journal of Management Information Systems* 31.3, pp. 7–34. DOI: 10.1080/07421222.2014.994672. eprint: https://doi.org/10.1080/07421222.2014.994672. URL: https://doi.org/10.1080/07421222.2014.994672.

Peter Mell, Timothy Grance (n.d.). *The NIST Definition of Cloud Computing*. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Pries-Heje, Jan and Richard Baskerville (2008). “The Design Theory Nexus.” In: *MIS Quarterly* 32.4, pp. 731–755. ISSN: 02767783. URL: http://www.jstor.org/stable/25148870.

PRISMA (n.d.). *TRANSPARENT REPORTING of SYSTEMATIC REVIEWS and META-ANALYSES*. URL: http://prisma-statement.org/prismastatement/flowdiagram.aspx. (accessed: 27.02.2021).

Rajaeian, Mohammad Mehdi, Aileen Cater-Steel, and Michael Lane (2017). “A systematic literature review and critical assessment of model-driven decision support for IT outsourcing.” In: *Decision Support Systems* 102, pp. 42–56. ISSN: 0167-9236. DOI: https://doi.org/10.1016/

j.dss.2017.07.002. URL: https://www.sciencedirect.com/science/article/pii/S0167923617301240.

Rajat Wason Shaun Aghili, Pavol Zavarsky (2020). *An Integrated CASB Implementation Model To Enhance Enterprise Cloud Security.*

Ramírez, Margarita Ramírez et al. (2016). “Information Technologies in the Area of Health and Use of Mobile Technologies in the Area of Health in Tijuana, Baja California.” In: *Innovation in Medicine and Healthcare 2016*. Ed. by Yen-Wei Chen et al. Cham: Springer International Publishing, pp. 129–134. ISBN: 978-3-319-39687-3.

Rittel, H.W.J. and M.M. Webber (1973). “Dilemmas in a general theory of planning.” In: *Policy Sci* 4, pp. 155–169. DOI: https://doi.org/10.1007/BF01405730.

Rizk, Dalia et al. (Nov. 2020). “A Study on Cloud Computing Architectures for Smart Healthcare Services.” In: *The 3rd International Conference on Informatics & Data-Driven Medicine*. Ed. by Nataliya Shakhovska et al. CEUR Workshop Proceedings, pp. 302–310.

Sein, Maung K et al. (2011). “Action Design Research.” In: *MIS Quarterly* 35.1, pp. 37–56. DOI: https://doi.org/10.2307/23043488.

Seixas, Brayan, Francois Dionne, and Craig Mitton (2021). “Practices of decision making in priority setting and resource allocation: a scoping review and narrative synthesis of existing frameworks.” In: *Health Economics Review* 11. DOI: https://doi.org/10.1186/s13561-020-00300-0.

Shackleford, Dave (2021). *SANS 2021 Cloud Security Survey*. URL: https://www.sans.org/reading-room/whitepapers/analyst/2021-cloud-security-survey-40225. (Accessed: 01.06.2021.

Shuaib, Mohammed et al. (Jan. 2019). “Why Adopting Cloud Is Still a Challenge?—A Review on Issues and Challenges for Cloud Migration in Organizations.” In: pp. 387–399. DOI: 10.1007/978-981-13-5934-7_35.

Sillic, Mario (2019). “Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow IT context.” In: *Computers & Security* 80, pp. 108–119. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2018.09.012. URL: https://www.sciencedirect.com/science/article/pii/S0167404818306114.

Spagnoletti, Paolo, Andrea Resca, and Øystein Sæbø (2015). “Design for social media engagement: Insights from elderly care assistance.” In: *The Journal of Strategic Information Systems* 24.2. Strategic and Policy Perspectives on Social Media Technologies, pp. 128–145. ISSN: 0963-8687. DOI: https://doi.org/10.1016/j.jsis.2015.04.002. URL: https://www.sciencedirect.com/science/article/pii/S0963868715000232.

Sykehuspartner (n.d.). *Om oss - Sykehuspartner*. URL: https://sykehuspartner.no/om-oss. (accessed: 21.05.2021).

Tam, Kenneth et al. (2013). “Chapter 1 - Introduction to UTM (Unified Threat Management).” In: *UTM Security with Fortinet*. Ed. by Kenneth Tam et al. Syngress, pp. 3–34. ISBN: 978-1-59749-747-3. DOI: https://doi.org/10.1016/B978-1-59-749747-3.00001-6. URL: https://www.sciencedirect.com/science/article/pii/B9781597497473000016.

Tervoort, Tom et al. (2020a). “Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review.” In: *IEEE Access* 8, pp. 84352–84361. DOI: 10.1109/ACCESS.2020.2984376.

— (2020b). “Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review.” In: *IEEE Access* 8, pp. 84352–84361. DOI: 10.1109/ACCESS.2020.2984376.

Thienen, Julia von, Christoph Meinel, and Claudia Nicolai (2014). “How Design Thinking Tools Help To Solve Wicked Problems.” In: *Design Thinking Research: Building Innovation Eco-Systems*. Ed. by Larry Leifer, Hasso Plattner, and Christoph Meinel. Cham: Springer International Publishing, pp. 97–102. ISBN: 978-3-319-01303-9. DOI: 10.1007/978-3-319-01303-9_7. URL: https://doi.org/10.1007/978-3-319-01303-9_7.

Twum, Frimpong, J. B., and J. K. (Jan. 2020). “A Comparative Study of Existing Cloud Security System Models as against an Implementation of the CDDI Model Dubbed SecureMyFiles System.” In: *International Journal of Computer Applications* 177, pp. 17–37. DOI: 10.5120/ijca2020919765.

Vandermarliere, Thomas (2016). *Protecting Enterprise Data in the Cloud*. URL: https://libstore.ugent.be/fulltxt/RUG01/002/300/734/RUG01-002300734%5C_2016%5C_0001%5C_AC.pdf. (Accessed: 01.06.2021).

Varonis, Jeff Petters - (2020). *What is UEBA? Complete Guide to User and Entity Behavior Analytics*. URL: https://www.varonis.com/blog/user-entity-behavior-analytics-ueba/. (accessed: 26.03.2021).

von Solms, Rossouw and Johan van Niekerk (2013). “From information security to cyber security.” In: *Computers & Security* 38. Cybercrime in the Digital Economy, pp. 97–102. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2013.04.004. URL: https://www.sciencedirect.com/science/article/pii/S0167404813000801.

Wells, Alex (2020). *What is Adaptive Access Control*. URL: https://www.wandera.com/adaptive-access-importance/. (accessed: 15.04.2021).