The factors determining cloud platform adoption

An exploratory study of the Dutch financial sector using the Best-Worst Method (BWM)

EPA MSc Thesis

J.B. (Iven) Stam

TU Delft

The factors determining cloud platform adoption

An exploratory study of the Dutch financial sector using the Best-Worst Method (BWM)

by

J.B. (Iven) Stam

Student Name	Student Number
J.B. (Iven) Stam	4606523

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on Monday May 15, 2023 at 14:15.

Chair & Second Supervisor:	J. (Jafar) Rezaei
First Supervisor:	Dr.ir. Z. (Zenlin) Roosenboom-Kwee
Company First Supervisor:	Stef de Goede
Company Second Supervisor:	Rose Stroo
Project Duration:	November, 2022 - April, 2023
Faculty:	Faculty of Technology, Policy and Management, Delft

Cover: FinTech Image mobibiz, 2019

TU Delft

Preface

This thesis is written as part of the 21-week MSc Thesis requirement for the *Engineering and Policy Analysis (EPA)* program at the *TU Delft Faculty of Technology, Policy and Management (TPM)*. During the duration of my thesis, I also completed a thesis internship at collaborating partner *Ernst and Young's (EY) FSO Tech Consulting*. The expertise and resources of EY were utilized during the course of this thesis.

From the TU Delft, I first want to thank my first supervisor *Dr.ir. Z. (Zenlin) Roosenboom-Kwee* for her excellent guidance throughout my thesis process. Second, I want to thank my second supervisor and chair *J. (Jafar) Rezaei* for his help and expertise on the Best Worst Method (BWM). I am grateful for their guidance during my thesis. From EY, I want to thank my counselor *Stef de Goede* and my buddy *Rose Stroo*. I am grateful for their support during my thesis internship at EY. Finally, I would also like to thank the 13 IT/Cloud experts who participated in interviews for my thesis. Transferring their valuable knowledge in the interviews ultimately contributed greatly to the results of this research.

J.B. (Iven) Stam
Delft, April 2023

Executive summary

The financial industry has been significantly transformed by innovations, but large financial institutions have managed to maintain their dominant position without implementing many innovations. However, new technologies have caused a shift and should no longer be ignored. They are now facing competition from high-tech newcomers, also known as Fin- or BigTechs, that threaten their dominance. A recent study shows that financial institutions have a growing interest in (cloud) platform business models (Fintechs) without being handled in a responsible way. Firms are under pressure to transform, but guidance on how to design and control this transformation is hard to find. EU regulators are concerned about the speed and scale at which financial institutions are moving critical functions and market operations to a few cloud platforms and they will soon have to demonstrate their ability to recover from a cyber-attack. Choosing a secure cloud platform is essential, but the complexity, risks and regulation make this decision-making process challenging.

There is a lot of literature available on cloud platform comparisons, adoption factors, and barriers to adoption in the financial sector, but these areas have never been combined to investigate the suitability of a cloud platform in the Dutch financial sector. This makes it difficult for these financial institutions to choose a suitable cloud platform. An in-depth study is needed to investigate the factors that influence the choice of a cloud platform. This research focuses primarily on cloud technologies, specifically the three dominant cloud platforms: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. In addition, the focus is only on the financial sector in the Netherlands, where the strict regulations in the field of privacy and security are interesting for this thesis topic.

In the end, this study aims to identify the key factors influencing the adoption of cloud platforms within the Dutch financial sector and determine the most suitable Cloud platform for this sector. Identifying these key factors will contribute to financial institutions' understanding of cloud technologies and assist in their decision-making process. Ultimately, this research will help prevent potential irregularities such as cyber-attacks and data leakages.

Based on the knowledge gap and the aim of this research, the following main research question is formulated:

What are the key influencing factors that determine the adoption of a cloud platform within the cloud platform battle within the Dutch financial sector?

To answer this main research question, several sub-questions are formulated:

1. What is the current state of Cloud in the Dutch financial sector?
2. What policy regulations currently affect the adoption of cloud platforms technologies in the Dutch financial sector?
3. What are relevant factors for the adoption of cloud platforms in the Dutch financial sector?
4. What are the most important factors for the adoption of a cloud platform, using the Best-Worst Method?
5. Which cloud platform is the most suitable for the Dutch financial sector?

To answer these questions, the Best-Worst Method is used to determine the key factors and the most suitable cloud platform. As the focus is on standard selection, a modified version of van der Kaa's 2011 framework was eventually chosen to identify the most important factors in this battle. Data is collected through literature reviews and expert interviews. 13 IT/Cloud experts are interviewed from various Dutch financial institutions, varying from the consulting, banking, insurance, government and academic sectors.

To determine the current state of cloud technology in the Dutch financial sector, a literature review and exploratory interviews with IT/Cloud experts was conducted. The results show that the global cloud platform market in the financial sector is expected to grow significantly, with currently AWS (Amazon) as the market leader, followed by Azure (Microsoft), and Google as a distant third. In the Dutch financial

sector, Azure and AWS have almost equal market shares (+/- 40%) while Google has a smaller market share (+/- 15%) . Larger financial institutions tend to use Azure, while smaller ones use AWS and Google more frequently.

The second sub-question aimed to identify policy regulations that affect the adoption of cloud platforms in the Dutch financial sector. The study found that financial institutions need to comply with various regulations, including GDPR, NISD, ISO standards and DORA. ESMA also published nine guidelines for financial institutions outsourcing to cloud service providers to ensure compliance and security.

The third sub-question aims to determine relevant factors for cloud platform adoption in the Dutch financial sector. From the 29 factors in the framework, the 24 most relevant were selected and five additional specific Cloud platform factors were added. This resulted in a new set of 29 factors relevant to Cloud platform adoption

Thirteen IT/Cloud experts were interviewed in sub-question four to determine the most important factors for cloud platform adoption within the Dutch financial sector, using the Best-Worst Method. The results show that the key factors were identified as *Security & Privacy*, *Brand Reputation and Credibility*, *Pricing Strategy*, *Commitment*, and *Compatibility*. From a regulator's perspective, *Security & Privacy* are top priorities, while *Brand Reputation and Credibility* are important for gaining trust in the cloud provider. *Pricing Strategy* is important for gaining power and negotiating for the long term, *Commitment* is crucial for partnership reliability, and *Compatibility* with existing infrastructure makes integration smoother.

Sub-question five aimed to determine which cloud platform is most suitable for the Dutch financial sector. The experts scored the three most popular cloud platforms (AWS, Azure, and Google) on each factor using the Best-Worst Method. The scores were then multiplied by factor weights found in the previous sub-question to arrive at the weighted scores per cloud platform on a given factor. The total weighted score per platform was then calculated, with Azure having the highest score and being the most suitable for the Dutch financial sector, followed by AWS in second place and Google in last place. However, large Dutch international financial institutions often opt for a multi-cloud strategy to reduce their dependence on a single provider and make it easier to switch providers when needed.

In summary, the research identified the key influencing factors determining the adoption of a cloud platform within the Dutch financial sector as *Security & Privacy*, *Brand Reputation and Credibility*, *Pricing Strategy*, *Commitment*, and *Compatibility*. Microsoft Azure was found to be the most suitable cloud platform for the Dutch financial sector, although larger institutions tend to use a multi-cloud strategy to guarantee independence.

This research contributed to previous literature on cloud platform adoption in several ways. First, the study built on a framework by van der Kaa and added five new factors related to cloud platform adoption. Second, the BWM approach was used for the first time to identify the key factors for cloud platform adoption and to compare cloud platforms based on the listed factors. Third, the three most popular cloud platforms (AWS, Azure, and Google) were quantitatively compared on every relevant factor found. Last, the combination of relevant factors and comparison of cloud platforms can help to specifically compare cloud platforms for a particular sector.

The research also has practical contributions that can benefit policymakers, financial institutions, and cloud providers. First, policymakers can use the research to adjust regulations for cloud providers to meet the found key factors for financial institutions, and to ensure compliance with regulations. Second, financial institutions can use the research to get an overview of related policies, identify the most relevant factors for choosing a cloud provider, and make a choice among the three popular cloud platforms. Third, the proposed framework can also be used to compare other cloud platforms and help government agencies test new cloud providers on the market. Finally, cloud providers can use the factors identified in the framework to develop successful strategies for entering the Dutch financial market.

Contents

List of Figures

List of Tables

Nomenclature

Abbreviations

Abbreviation	Definition
AFM	Authority Financial Markets
AMLD	Anti-Money Laundering Directive
API	Application Programming Interface
AWS	Amazon Web Services
BWM	Best-Worst Method
CapEx	Capital Expenditure
Colo	Co location
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CSP	Cloud Service Provider
DevOps	Software development and IT Operations
DNB	The Dutch Central Bank
DORA	Digital Operational Resilience Act
DPO	Data Protection Officer
EPA	Engineering and Policy Analysis
ESMA	European Securities and Markets Authority
EU	European Union
EY	Ernst and Young
FinTech	Financial Technology
FSO	Financial Services Organisation
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
IoT	Internet of Things
ISO	International Organisation for Standardization
MCDM	Multi-Criteria Decision-Making
MiFID	Markets in Financial Instruments Directive
NAS	Network-attached Storage
NIC	Network Interface Card
NISD	Network and Information Systems Directive
NIST	National Institute of Standards and Technology
OpEx	Operational Expenditure
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
PSD2	Payment Services Directive 2
PSPs	Payment Service Providers
RAM	Random Access Memory
SaaS	Software as a Service
SAN	Storage Area Network
SLA	Service Level Agreement
SQS	Simple Queue Service
TCO	Total Cost of Ownership
VPC	Virtual Private Cloud
VPN	Virtual Private Network
Wft	Financial Supervision Act

Abbreviation	Definition
Wwft	Anti-Money Laundering and Counter-Terrorism Financing Act
XaaS	Anything as a Service

1 Introduction

This chapter will first introduce the topic with some background information. Second, the problem will be identified by discussing the knowledge gap, scope, societal and scientific relevance. Third, the research objectives will be discussed, resulting in the main and sub research questions. Lastly, the outline of the thesis is presented.

1.1. Background information

Over the past two decades, innovations have significantly transformed many industries, including the financial sector. However, traditional banks have been able to maintain their dominant position without implementing many innovations, mainly due to the high levels of regulation acting as a barrier to entry (Gutierrez, 2019). In addition, traditional banks are hesitant to innovate due to their need to comply with numerous financial and privacy regulations, the complexity of their services/products, and the trust issues involved in handling people's money (Hurwitz, 2019). However, new technologies such as cloud, block chain, and cross-border payments have caused a shift in the industry and can no longer be ignored (Gomber et al., 2018). These technologies have changed everything, and banks are now facing the arrival of high-tech new competitors, also known as FinTech or BigTech, that threaten their dominance (Gutierrez, 2019). The sector is digitizing, and large financial firms need to get involved to meet customer needs. Traditional systems must be overhauled, and current characteristics that form the biggest barriers to innovation must be investigated. A recent study shows that large financial firms have a growing interest in (cloud) platform business models without being handled in a safe way (Das, 2019). Firms are under pressure to transform, but proper guidance on how to design and control this is hard to find (Das, 2019). Financial institutions worldwide are also increasingly adopting cloud services from BigTechs (Brits et al., 2021). These services help increase their innovativeness, flexibility, and efficiency, but there are also concerns about data sovereignty, data privacy, operational resilience, and security (Brits et al., 2021). The global financial cloud market is expected to grow from $24 billion in 2022 to $90 billion in 2032 (FMI, 2021). This is a significant growth and EU regulators worry about the speed and scale at which financial institutions are moving critical functions and market operations onto a handful of cloud platforms (Jones, 2022). Financial institutions in the European Union will soon have to show how they can recover from a cyber attack as they increasingly rely on cloud giants such as Amazon, Microsoft, Google, and IBM for their main services (Jones, 2022). Currently, there are three BigTech parties dominating the cloud services market, namely Amazon Web Services (AWS), Microsoft Azure, and Google Cloud (Brits et al., 2021). The three services have similarities, but also differ in certain aspects. Choosing a secure cloud platform is crucial, but the complexity, risks and regulation make this decision-making process challenging.

1.2. Problem identification

In this section, the research problem will be identified. First, the knowledge gap will be discussed. Then the research scope will be given and finally the societal and scientific relevance will be discussed.

1.2.1. Knowledge gap

The global financial cloud market has experienced significant growth in recent years and this trend is expected to continue (FMI, 2021). This growth has made it necessary for financial institutions in the Netherlands to adopt this technology in order to meet customer needs (Gomber et al., 2018). However, a recent study reveals that large financial companies are increasingly interested in (cloud) platform business models without taking adequate security measures (Das, 2019). Companies are under pressure to transform, but there is limited guidance on how to design and control these processes (Das, 2019). Furthermore, EU regulators are concerned about the rapid and widespread adoption of cloud platforms by banks, insurers, and investment firms (Jones, 2022). Financial institutions in the European Union will soon have to demonstrate their ability to recover from irregularities, such as cyber attacks or data leakages, as they increasingly rely on cloud services (Jones, 2022). The literature review indicates that there is ample literature on cloud platform comparisons, adoption factors, and barriers to adoption in the financial sector, but these three areas have never been combined to examine the potential suitability of a cloud platform in the Dutch financial sector. For Dutch financial institutions, choosing a secure cloud platform is critical, but the complexity of the technology and regulation of the sector makes this decision-making process challenging. Based on this information, the following knowledge gap has been identified: there is currently little to no research on the key factors that determine which cloud platform is the most suitable in the Dutch financial sector. This sector is subject to many national and international (EU) regulations, which complicate the decision-making process for such a cloud platform.

1.2.2. Scoping

In order to make this research feasible, the scope of the topic needs to be defined. It is not possible to investigate all aspects of the topic in the time span of this research, so choices must be made.

First of all, this thesis will primarily focus on cloud technologies. While there are several emerging technologies, I have chosen to focus on the cloud as it is a current hot topic of interest within the industry and for regulators and the global financial cloud market is expected to grow from $24 billion in 2022 to $90 billion in 2032 (FMI, 2021). Additionally, I have decided not to include all cloud platforms in this research. Instead, I will focus on the three most dominant cloud platforms worldwide today: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud (Brits et al., 2021).

Second, this research will focus on the financial sector. This choice is based on the fact that this sector is bound by specific regulations in the field of privacy and security (Gutierrez, 2019), which can have an impact with regard to this thesis topic. Other sectors don't have or have adjusted these regulations, so the outcome may be interesting.

Last, the geographical focus will be on the Netherlands. This choice is due to the fact that regulations in the financial sector can vary greatly between countries and my geographical location makes it more accessible to talk to institutions in this area.

In conclusion, the scope of this research will be focused on the three main cloud platforms (AWS, Azure, and Google) within the Dutch financial sector.

1.2.3. Societal and scientific relevance

Cloud technology is becoming increasingly crucial in the modern workplace, including the financial sector. Financial institutions must adopt cloud platforms to remain competitive. Customers have ever increasing high demands on IT systems, such as inter banking, and must be kept satisfied with modern systems. The significance of this topic is considerable and will be demonstrated in this section. Firstly, the scientific relevance will be explored, followed by the societal relevance.

Scientific relevance

From a scientific standpoint, this topic is highly relevant. The literature review reveals that there is a significant amount of literature available on this topic, indicating its scientific relevance. The literature can be divided into three main categories: cloud platform comparison, cloud adoption factors, and barriers cloud adoption in the financial sector. Below we briefly discuss each category.

- **Cloud platform comparison:** This category includes studies that have examined the differences between the dominant cloud platforms. A literature review reveals that approximately five articles have conducted comparative analyses of Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.

In 2018, Kotas et al. compared Amazon Web Services and Microsoft Azure on their compute-oriented instances (Kotas et al., 2018). In 2019, Opara compared four popular cloud platforms, including AWS, Microsoft Azure, Google App Engine, and IBM Cloud, on common features such as cloud service type, storage, and database (Opara, 2020). In 2021, Kaushik et al. conducted a study on the architecture and types of cloud computing services, which also compared the performance and service of AWS, Microsoft Azure, and Google Cloud Platform (Kaushik et al., 2021). In 2020, Wankhede et al. conducted a comparative analysis of the three main cloud platforms in terms of pricing, specifications, support and administration (Wankhede et al., 2020). Lastly, in 2019, Pierleoni et al. conducted a study comparing the services available for IoT on the three main cloud platforms (Pierleoni et al., 2020).

The numerous recent papers on this topic demonstrate the scientific relevance and highlight the knowledge gaps. Currently, there is a lack of research on the differences between the main cloud platforms (Amazon AWS, Microsoft Azure, and Google Cloud) in the financial sector. Therefore, the knowledge gap primarily concerns this sector, as it offers unique products and is subject to specific regulations (Gutierrez, 2019). It would be interesting to examine the differences between cloud platforms in this sector

- **Cloud adoption factors:** This category encompasses the studies that have investigated the factors influencing the adoption of cloud technologies/platforms within companies or institutions. The literature review reveals that eight papers have conducted research on these factors.

  Asatiani conducted a study in 2015 on the adoption factors that influence an organization's decision to adopt cloud technology (Asatiani, 2015), while Hsu and Lin used the technology-organization-environment framework to investigate factors influencing the adoption of cloud computing services (Hsu and Lin, 2016). Singh et al. explored the factors that influenced the adoption of cloud computing technologies in the banking sector (Singh et al., 2018), and Asadi et al. proposed an adoption model based on the TAM-diffusion theory model from a customer perspective in the banking sector (Asadi et al., 2017). Morgan and Conboy's 2013 study addressed the complex and multifaceted nature of cloud adoption (Morgan and Conboy, 2013), and Rai et al. comprehensively identified, categorized, and compared existing research on legacy to cloud migration in 2015 (Rai et al., 2015). Werth et al. used qualitative research to examine the factors that influence digital transformation in the financial services sector in 2020 (Werth et al., 2020). Kuiper et al. conducted a study in 2022 exploring the factors that impact cloud adoption in the public sector (Kuiper, 2014).

  Overall, there is a wealth of literature on the scientific relevance of this topic, but few, if any, papers have specifically addressed the factors influencing the potential suitability and adoption of a cloud platform in the Dutch financial sector.

- **Barriers cloud adoption:** This category pertains to the challenges faced by financial institutions in adopting cloud technology. The literature review reveals that four papers have studied these barriers.

  In 2018, Alsmadi and Prybutok conducted a study on cloud sharing and storage behavior and the contradiction between industry reports and academic cloud adoption literature (Alsmadi and Prybutok, 2018). In 2019, Scott et al. analyzed the use of cloud computing in the financial industry and current regulations and supervision for cloud usage (Scott et al., 2019). In 2022, Sathye and Bhardwaj published a paper discussing the challenges financial firms face when adopting mobile cloud computing (Sathye et al., 2022). Also in 2022, Stewart created a model to identify challenges and specific implications preventing the adoption of cloud technology in Germany (Stewart, 2021).

  Based on this research, it can be concluded that a lot of work has been done on the barriers to cloud technology adoption in financial institutions, indicating the scientific importance of this topic. However, little or no research has been done on the challenges that play a role in choosing a cloud platform in the Dutch financial sector. Cloud technologies and platforms can vary greatly and therefore score differently on certain factors.

Overall, there is a wealth of literature available on the topics of cloud platform comparisons, cloud adoption factors, and barriers to cloud adoption in the financial sector, indicating the scientific relevance of this topic. However, these areas of knowledge have never been combined to investigate the potential

suitability of a cloud platform in the Dutch financial sector. This makes it difficult for financial institutions in the Netherlands to choose a suitable cloud platform to implement in their business. These institutions would like to implement (cloud) platform business models, but often do not know how to design and control them effectively (Das, 2019). Therefore, an in-depth study is needed to investigate the factors that influence the choice of a cloud platform and how it can be implemented in an ethical and secure manner. The increasing threats to cybersecurity and privacy should also be considered in this research.

Societal relevance

From a societal perspective, identifying key factors that determine the suitability of a cloud platform within the Dutch financial sector will contribute to financial institutions' understanding of cloud technologies. As identified in the problem definition, it is currently difficult for these institutions to choose a suitable cloud platform for their specific services due to the complexity of cloud technology, the large number of platforms, and regulations. This research will ultimately assist these institutions in their decision-making process and can prevent potential irregularities such as cyber-attacks and data leakages. Overall, this research will contribute to the decision process of choosing a cloud platform and can help prevent potential irregularities.

1.3. Research objectives and questions

After conducting a literature review, it was determined that there is a lack of understanding regarding the implementation of complex innovations, such as cloud platform business models, at financial institutions. This study aims to gain insight into the key factors that influence the adoption of a cloud platform within the Dutch financial sector. By considering the unique characteristics and regulations of this industry and identifying the key factors of influence, this research aims to identify a suitable cloud platform.

Based on the knowledge gap, the following main research question was formulated:

What are the key influencing factors that determine the adoption of a cloud platform within the cloud platform battle within the Dutch financial sector?

To answer this main research question, several sub-questions have been formulated:

1. What is the current state of Cloud in the Dutch financial sector?
2. What policy regulations currently affect the adoption of cloud platforms technologies in the Dutch financial sector?
3. What are relevant factors for the adoption of cloud platforms in the Dutch financial sector?
4. What are the most important factors for the adoption of a cloud platform, using the Best-Worst Method?
5. Which cloud platform is the most suitable for the Dutch financial sector?

The findings from each sub-question serve as the input for the subsequent sub-question and will ultimately provide an answer to the main research question.

Ultimately, the aim of this study is to determine the most suitable cloud platform for the Dutch financial sector. To achieve this, a quantitative approach was adopted, using the Multi-Criteria Decision-Making (MCDM) approach and the Best-Worst Method (BWM) to identify the key factors that are of main influence on this battle within this sector. Using the same method and factors, the characteristics of the cloud platforms were compared with each other, resulting in the platform that has the greatest potential to be the most suitable for this sector. This method was chosen for its ability to effectively solve MCDM problems in a simple way with fewer pairwise comparisons, more reliable weights and less comparison data than other MCDM-methods (Rezaei, 2015). The results of this quantitative approach will help determine which platform has the greatest potential in the sector. Ultimately, this research will contribute to our understanding of the adoption of cloud platform models in the financial industry.

1.4. Thesis outline

This paper will first discuss the research methodology in chapter 2. This covers the chosen framework, method and interview setup. Secondly, the theoretical background will be explained in chapter 3. This includes the literature review, general introduction to cloud and policy arena. Thirdly, the relevant factors

will be discussed in Chapter 4. The categories and associated factors will be explained here. Fourthly, the results, associated analyses and the discussion of these results will be discussed in Chapter 5. Finally, chapter 6 will answer the research questions, but will also reflect and make recommendations for future research.

2

Research methodology

Chapter 1 discussed that the Multi-Criteria Decision-Making (MCDM) approach is used for solving the issue. This chapter will first determine which conceptual framework and MCDM method are most appropriate. Second, the data, research methods, and tools needed for each sub-question will be discussed. Third, the overall research design will be presented in a flow diagram and finally, the interview setup is presented.

2.1. Conceptual framework and method selection

This paper, as mentioned in Chapter 1, will explore the key factors that affect the cloud platform adoption in the Dutch financial cloud platform battle. In order to address this question, a conceptual framework and methodology must be selected. This section first provide a brief overview of the various conceptual frameworks and finally discuss the different MCDM methodologies. After each section, a conclusion is made on which framework or method is most suitable for this research.

2.1.1. Conceptual framework

Only a few frameworks have been created to study the factors that influence the outcome of a technology battle. Suarez developed one of the first frameworks in 2004 and identified eight key factors that can be divided into two categories: environmental and firm-level factors (Suarez, 2004). These factors were later expanded upon by Van der Kaa et al. in 2011, who identified a total of 29 factors (van de Kaa et al., 2011). These factors were divided into five categories: characteristics of the format supporter, characteristics of the format, format support strategy, other stakeholders, and market characteristics. This study will focus on examining the battle between the three largest cloud platforms (AWS, Azure, and Google Cloud) and determine which platform is the most suitable for the Dutch financial sector. Because Van der Kaa et al.'s framework is applicable to all kind of technology battles, it is also highly standardized. To make it more applicable to this particular Cloud platform battle, I chose to use exploratory expert interviews and a literature review to filter the 29 factors for relevance and possibly add new relevant factors.

Since the focus is on standards selection, a modified version of van der Kaa's 2011 framework (van de Kaa et al., 2011) was ultimately chosen to identify the key factors in this battle. From the 29 factors in the framework, the most relevant ones for this thesis topic were selected and additional specific Cloud platform factors were added.

2.1.2. Method

In this research, I have chosen to use a Multi-criteria decision-making (MCDM) approach. This is a decision-making process that requires consideration of multiple criteria, in this case factors. This method aims to select the best alternative from a set of available alternatives evaluated on the basis of multiple criteria. The different criteria are evaluated and then given a weight according to their importance. In the end, the best alternative can be selected that has the highest summed weight on the desired criteria. This study investigates which cloud platform is most suitable for the Dutch financial

sector and thus meets the desired criteria for this sector, making the MCDM approach very suitable for this study.

There are many methods for solving MCDM problems, but the most popular ones are the Analytic Hierarchy Process (AHP) (R. W. Saaty, 1987), Analytic Network Process (ANP) (T. L. Saaty and Vargas, 2013), Choosing By Advantages (CBA) (Suhr, 1999), and Best Worst Method (BWM) (Rezaei, 2015). In this research, I have decided to use the Best Worst Method, which was developed by Jafar Rezaei (Delft University of Technology) in 2015 (Rezaei, 2015). This method is a MCDM where the decision-maker describes their preferences by comparing the different factors, also known as pairwise comparison (Rezaei, 2015). Two pairwise comparison vectors (Best-to-other and Others-to-Worst) are chosen as input for an optimization model to get the optimal weights for the criteria. This method is more suitable than the other methods because it requires fewer pairwise comparisons and gives more reliable weights (Rezaei, 2015). This will make it easier for experts to participate in the interviews. In addition, it needs less comparison data and is simpler, because only integer numbers between one and nine are used instead of matrices with integers and fractional numbers (Rezaei, n.d.). As a result, fewer interviews with experts will have to be conducted than with other MCDM methods and analyzing the results will be easier.

Best-Worst Method

As mentioned in the previous section, the BWM approach will be used to compare the different categories, their associated factors and three most popular cloud platforms on these factors. The BWM is applicable to an MCDM problem. A typical MCDM problem can be seen in the matrix below:

$$A = \begin{array}{c} \\ a_1 \\ a_2 \\ \vdots \\ a_m \end{array} \begin{array}{c} \begin{array}{cccc} c_1 & c_2 & ... & c_n \end{array} \\ \begin{pmatrix} p_{11} & p_{12} & ... & p_{1n} \\ p_{21} & p_{22} & ... & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{m1} & p_{m2} & ... & p_{mn} \end{pmatrix} \end{array}$$

In the matrix above,$\{a_1, a_2, ..., a_m\}$ is a set of feasible alternatives that can be considered solutions and $\{c_1, c_2, ..., c_n\}$ is a set of decision-making criteria. The values within the matrix represent the performance scores of alternative *i* on criterion *j* as p_{ij}. The goal is to select the best (most suitable) alternative, in other words an alternative with the best overall value. The overall value of alternative *i*,V_i can be obtained using various methods. In a general form, if we assign weight $w_j (w_j \geq 0, \sum w_j = 1)$ to criterion *j*, then V_i can be obtained using a simple additive weighted value function, which is the underlying model for most MCDM methods, as follows:

$$V_i = \sum_{j=1}^{n} w_j p_{ij}$$

This BWM consists of five steps (Rezaei, 2015, 2016) which are further explained below:

- **Step 1:** Determine the set of decision criteria. The decision-maker identifies *n* criteria $\{c_1, c_2, ..., c_n\}$ that are used to make a decision.
- **Step 2:** Determine the best (most important) and worst (least important) criterion within a given category.
- **Step 3:** Determine the preference of the best criterion over all the other criteria, using a number between 1 and 9. The resulting Best-to-Others (BO) vector would be: $A_B = (a_{B1}, a_{B2}, ..., a_{Bn})$, where a_{Bj} indicates the preference of the best criterion *B* over criterion *j*. It is clear that $a_{BB} = 1$.
- **Step 4:** Determine the preference of all the criteria over the worst criterion, using a number between 1 and 9. The resulting Others-to-Worst (OW) vector would be: $A_W = (a_{1W}, a_{2W}, ..., a_{nW})^T$, where a_{jW} indicates the preference of the criterion *j* over the worst criterion *W*. It is clear that $a_{WW} = 1$.

- **Step 5:** Find the optimal weights $(w_1^*, w_2^*, ..., w_n^*)$. The aim is to determine the optimal weights of the criteria, such that the maximum absolute differences $|w_B - a_{Bj}w_j|$ and $|w_j - a_{jW}w_W|$ for all *j* is minimized, which is translated to the following mathematical model:

$$minmax_j\{|w_B - a_{Bj}w_j|, |w_j - a_{jW}w_W|\}$$

such that

$$\sum_j w_j = 1,$$
$$w_j \geq 0, \text{for all } j.$$

This can be translated in the linear model below:

$$min\xi,$$

such that

$$|w_B - a_{Bj}w_j| \leq \xi, \text{for all } j,$$
$$|w_j - a_{jW}w_W| \leq \xi, \text{for all } j,$$
$$\sum_j w_j = 1,$$
$$w_j \geq 0, \text{for all } j.$$

Solving the model results in the optimal weights $(w_1^*, w_2^*, ..., w_n^*)$ and ξ^*.

- **Step 6:** Calculate the consistency ratio by making use of the following formulas for input based BWM (Liang et al., 2020):

$$CR = max_j CR_j$$

where

$$CR_j = \begin{cases} \frac{|a_{Bj} * a_{jW} - a_{BW}|}{a_{BW} * a_{BW} - a_{BW}}, & a_{BW} > 1 \\ 0, & a_{BW} = 1 \end{cases}$$

The calculated consistency ratio is then compared to the threshold values presented in Table 2.1 (Liang et al., 2020).

Table 2.1: Threshold for the consistency ratio for input-based (Liang et al., 2020)

Scale	Criteria						
	3	**4**	**5**	**6**	**7**	**8**	**9**
3	0.1667	0.1667	0.1667	0.1667	0.1667	0.1667	0.1667
4	0.1121	0.1529	0.1989	0.2206	0.2527	0.2577	0.2683
5	0.1354	0.1994	0.2306	0.2546	0.2716	0.2844	0.2960
6	0.1330	0.1990	0.2643	0.3044	0.3144	0.3221	0.3262
7	0.1294	0.2457	0.2819	0.3029	0.3144	0.3251	0.3403
8	0.1309	0.2521	0.2958	0.3154	0.3408	0.3620	0.3657
9	0.1359	0.2681	0.3062	0.3337	0.3517	0.3620	0.3662

This study uses a BWM-solver in Excel that automatically solves the model based on the experts' preferences. The consistency ratio, which evaluates the consistency level of the experts' comparisons and the reliability of the weights, is represented in the Excel file as Input-based CR and ranges from 0 to 1. The recent study by Liang et al. proposed threshold values for different combinations of criteria and scale to determine the acceptability of the consistency ratio (see Table 2.1), where the ratio must be below or equal to the corresponding threshold value to be acceptable (Liang et al., 2020). If not, the pairwise comparison is revised by the expert till the consistency ratio is acceptable.

2.2. Research steps

This section first discusses the data collection for each sub-question. Subsequently, these research steps will be summarized in a research flow diagram.

2.2.1. Data collection

This section discusses the data needed for each sub-question, the appropriate research methods to collect that data and the tools to analyse that data.

1. *What is the current state of cloud in the Dutch financial sector?*

   The goal of this sub-question is to learn more about the technology behind different cloud platforms and their current state within the Dutch financial sector. To do this, I will first collect data primarily from literature on cloud platform technologies and market insights. This literature may be general or specific to the implementation of these technologies within the financial sector. The advantages of this method are that there are many potentially interesting articles to be found via the internet. A disadvantage is the difficulty to find the appropriate information in the large number of articles. Second, I will also conduct exploratory interviews with cloud experts to gain a user perspective on the Dutch financial cloud market. The setup of the different interviews can be found in section 2.3. The data is collected by following structured interview questions and summarising their answers.

2. *What policy regulations currently affect the adoption of cloud platforms technologies in the Dutch financial sector?*

   This sub-question focuses on the policy landscape in which the battle for cloud adoption in the financial sector takes place. As is well known, financial institutions in the EU are subject to a number of regulations, which may impact the implementation and choice of a cloud platform. The aim of this question is to identify these regulations and assess their potential influence on the implementation and choice of a cloud platform.

   To collect data for this sub-question, I primarily relied on literature on regulations within financial firms. This can include general literature on technology regulation or specific regulations on cloud platforms. Articles related to tech and/or cloud regulation within financial services are reviewed and collected. One advantage of this method is that there are many potentially interesting articles available online. However, a disadvantage is the difficulty in finding the appropriate information among the large number of articles. As in sub-question one, I also used exploratory interviews as a source of information for this sub-question. During the interviews, experts were asked about the regulations that currently exist within the financial sector and their potential impact on the adoption of cloud platforms. The setup of the interviews is described in section 2.3. To subsequently analyze the data, The data is collected by following structured interview questions and summarize their answers.

3. *What are relevant factors for the adoption of cloud platforms in the Dutch financial sector?*

   The aim of this sub-question is to identify the key factors influencing the competition between cloud platforms in the Dutch financial sector. The data for this study was first gathered through a literature review. This literature review provided a base framework of factors, which was refined through the interviews. In the process of defining key factors, the framework of factors from van de Kaa and de Vries (van de Kaa et al., 2011) was used as a basis. The advantages and disadvantages of using a literature review and expert interviews were considered. Second, exploratory interviews with industry experts were conducted to collect data. See section 2.3 for the setup of the expert interviews. The data is collected by following structured interview questions and summarize their answers.

4. *What are the most important factors for the adoption of a cloud platform, using the Best-Worst Method?*

   This sub-question has the goal to identify the key factors that contribute to the adoption of a cloud platform within the Dutch financial sector. The factors that are critical for financial institutions when selecting a cloud platform will be discussed, and data was collected from the BWM questions in the second round of interviews. In these interviews, the experts were asked to compare the categories and associated factors, using the Best-Worst Method (BWM) (see section 2.1.2). This ultimately resulted in optimal weights for each factor. The outcome is a ranking of the importance of the set of factors based on these weights. Finally, validation interviews were also conducted in the third round. Here, the results of this sub-question were presented and the experts were asked to validate and explain these results.

5. *Which cloud platform is the most suitable for the Dutch financial sector?*

   This sub-question has the goal to find the most suitable cloud platform for the Dutch financial sector. The data for this was obtained from the second round of interviews. In these interviews, experts were asked to compare the three most popular cloud platforms (AWS, Azure and Google) on each factor, using the Best-Worst Method (BWM) (see section 2.1.2). This ultimately resulted in optimal weights for each cloud platform on each factor. These weights can be seen as performance scores and by multiplying these scores by the optimal weights of each factor and summing them up, the final score for each platform was calculated. The higher the final score, the greater the chance the platform is more suitable for the Dutch financial sector. Finally, validation interviews were also conducted in the third round. Here, the results of this sub-question were presented and the experts were asked to validate and explain these results.

2.2.2. Research Flow Diagram

The figure below depicts the overall research design in a flow diagram. This schematic illustrates all research steps, sub-questions, research methods, and deliverables.

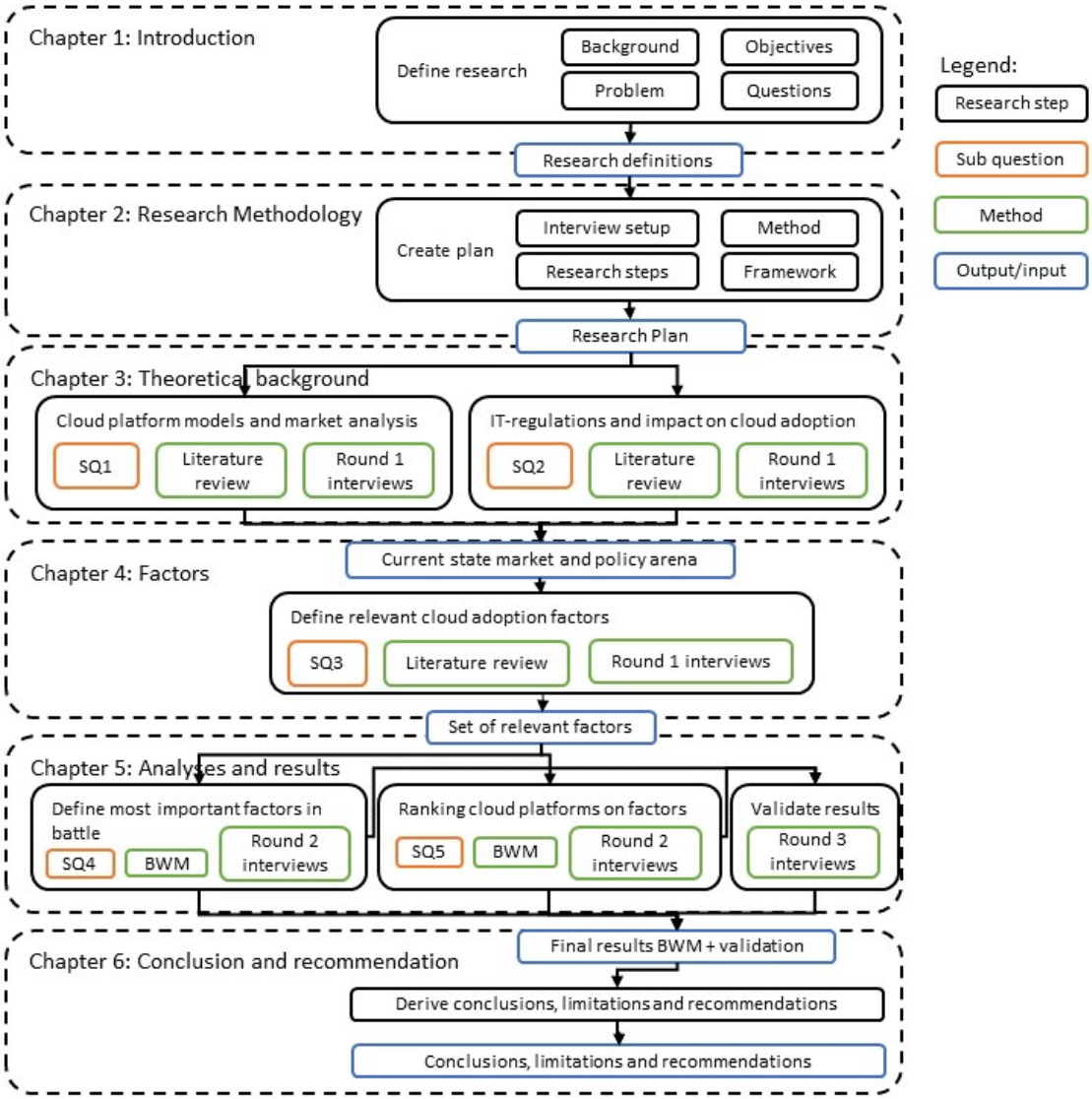

Figure 2.1: Research design

2.3. Interview setup

This section elaborates on the interviews conducted to answer certain sub-questions. First, the stakeholder analysis is briefly discussed with to show which specific sectors interviews were scheduled to get an overall picture of the Dutch financial sector. Then an overview of the interviews is given.

2.3.1. Stakeholder analysis

The financial sector is very important to the Dutch economy. In total, there are as many as 1400 financial institutions (DNB, n.d.). These are banks and insurers, but also pension funds, trust offices, crypto providers, payment service providers and investment institutions. In addition, there are also regulators, think of the DNB and AFM, consulting firms and knowledge institutes, such as universities, all involved in the financial sector.

Since this research aims at finding out the main factors for the adoption of cloud platforms, interviews will mainly be conducted with individuals with IT/Cloud knowledge within this sector. Using my own network and those of individuals around me, I ended up conducting interviews with IT/Cloud experts within the consulting, banking, insurance, government and academic sector.

2.3.2. Interview overview

In this section, the details of the interviews are presented in an overview. As mentioned in the previous section, three rounds of interviews are conducted - an exploratory, a BWM and a validation round. Each round focuses on answering specific sub-questions. The table below provides an overview of the sub-questions, topics, sectors, number of interviews, and expert expertise for each round.

Table 2.2: Interview setup overview

Round	Sub question	Topic(s)	Sector	Number of interviews	Expertise
1	1	- Core concepts cloud technologies - Current Cloud platform market in Dutch financial sector	Consultancy (Financial Sector)	2	Cloud technology
	2	- Regulations related to IT in the Dutch financial sector - Impact regulations on Cloud adoption			
	3	- Factors for adoption in cloud platform battle		1	IT/cloud Regulation
2	4	- Finding the key factors determine Cloud platform adoption, using BWM	Consultancy (Financial sector)	6	IT/Cloud Technology
			Banking	2	
	5	- Comparing Cloud platforms (AWS, Azure and Google) on factors	Insurance	3	
			Academic	1	
			Government	1	
3	4	- Validate key factors Cloud Platform adoption	Banking	2	IT/Cloud Technology
	5	- Validate Cloud platform comparison (AWS, Azure and Google)	Insurance	1	

First round

The first round of interviews, as indicated in Table 2.2, serves as input for sub-questions one, two, and three. This round is exploratory in nature and involves three interviews with experts within the Financial Services consultancy sector. In addition, they also have experience in other area's of the financial sector. See interviewees details below:

Table 2.3: Interview setup round 1

#	Background	Function	Expertise
1	Consultancy	Manager Technology Transformation	Cloud, IT transformation, IT Strategy
	Insurance	Manager Finance IT/Product-owner cloud	
2	Consultancy	Senior Manager Data & Analytics	Data management, BI, Data Science, Data Engineering
	Private equity	Intern	
3	Consultancy	Senior consultant	Agile Transformations, Business Development
	Cloud provider	Technical Specialist	

As mentioned in table 2.2, three different sub-questions are answered in this round of interviews. The interview questions are also categorized into these three different categories, i.e. general questions about the core concepts of cloud and the current market, questions about regulation and its impact on cloud adoption and questions about the relevance of factors. Beyond that, the interview started with general questions or the profile of the expert and his/her relationship to cloud. A complete overview of all interview questions can be found in appendix A.1.

Second round

The second round is more comprehensive and provides information for sub questions four and five. This round is crucial to the research and serves as the main source of data for the final results. In total, 13 interviews were conducted with experts from various sectors, including Consultancy, Banking, Insurance, regulator and academic. During these interviews, the factors identified in sub-question

three are compared by the experts using the Best Worst Method. Also the three most popular cloud platforms (AWS, Azure and Google) are compared on each factor using the same method. Based on these rankings and comparison of cloud platforms, a potential most suitable cloud platform within the Dutch financial sector is determined. See interviewees profiles in the table below.

Table 2.4: Interview setup round 2

#	Background	Function	Expertise
1	Consultancy	Manager Technology Transformation	Cloud, IT transformation, IT Strategy
	Insurance	Manager Finance IT/Product-owner cloud	
2	Consultancy	Senior Manager Data & Analytics	Data management, BI, Data Science, Data Engineering
	Private equity	Intern	
3	Consultancy	Senior consultant	Agile Transformations, Business Development
	Cloud provider	Technical Specialist	
4	Consultancy	Manager Cybersecurity	Cybersecurity, Emerging Tech, Cloud Transformation, IT Risk
5	Consultancy	Customer Director	Cloud Implementation, cloud strategy
6	Consultancy	Product Owner Cloud (in banking)	Backend competences, integrations, API, Databases, Cloud CRM integrations, CAP
7	Insurance	Security Analyst/ Architect/Engineer	Cloud onboarding, IT infrastructure, Data and eco-systems, IT security
8	Insurance	Manager IT	Infrastructure, Cloud Migrations, Hosting and movements to SaaS
9	Insurance	IT-Architect	IT Advising MT, Software development, Datacenters, Single sign-on features
10	Banking	Product Owner Cloud	Cloud journey, Vendor selection, Framework, Governance, IT-Security requirements
11	Banking	Solution Architect	Data/Cloud, AWS, Machine Learning, Azure
12	Regulator	Product Owner - Data and Reporting	Building data reals, Azure, Reporting automation
	Insurance	Product Owner - IFRS 17 Reporting and Consolidation	
13	Academic	Associate Professor Faculty Technology, Policy and Management, Head section ICT	Digital platforms, Data exchange, Software, ICT Architecting

As mentioned in table 2.2, two different sub-questions are answered in this round of interviews. The interview questions are also categorized into these two different categories, i.e. Questions about the categories with their factors and their comparison using the BWM and questions about the three platforms and their scores on the various factors also using the BWM. In addition, the interview also started with general questions or the profile of the expert and his/her relationship to cloud. A complete overview of all interview questions can be found in appendix A.2.

Third round

The third round of interviews serves more as a validation round. In this round, the final results of the BWM from the second round are validated. The purpose of these rounds is to find an explanation for the results and to correct possible misinterpretations or other details. A total of three different experts were interviewed, who also participated in the second round. See the interviewee's profiles below.

Table 2.5: Interview setup round 3

#	Background	Function	Expertise
1	Insurance	IT-Architect	IT Advising MT, Software development, Datacenters, Single sign-on features
2	Banking	Product Owner Cloud	Cloud journey, Vendor selection, Framework, Governance, IT-Security requirements
3	Banking	Solution Architect	Data/Cloud, AWS, Machine Learning, Azure

As explained in Table 2.2, this round serves as validation of the results of the answers to sub-questions 4 and 5. The interview questions are categorized into three different categories, namely general questions about the specific experts, validation questions about the BWM final factor results and validation questions about the platform comparison final results. A complete overview of all the interview questions can be found in appendix A.3.

3

Theoretical background

This chapter goes into further detail on the theoretical background of this research. First, the technology is further described, by going into the core concepts of Cloud, providing a market analysis and briefly describing the three most popular platforms. Next, the policy arena, in which the technology battle takes place, is discussed further. Important regulations will be named with their impact on the adoption of cloud platforms within the industry and finally the guidelines as a result.

3.1. Description of the technology

In this section, I will elaborate on the different aspects of Cloud technology. First, the core concepts of cloud are discussed. Next, a brief market analysis is done on cloud platforms in the global and Dutch financial sector and finally, the three most popular cloud platforms (AWS, Azure and Google cloud) are briefly explained.

3.1.1. Cloud technology

In this section, the core concepts of the cloud are discussed in more detail. First, the traditional deployment models before the introduction of the cloud are discussed. Second, the definition of cloud computing is given and the characteristics of the cloud are discussed. Third, the general benefits of cloud computing are given. Fourth, the different cloud implementation models are explained and, finally, the different cloud service models are discussed.

Traditional Deployment Models for IT Services

Before the emergence of cloud computing, companies had a few options for deploying IT services. These deployment models included on-premises solutions, colocation (also known as ”colo”) and server virtualisation (Anderson, 2021).

- **On-Premises Solutions:** With on-site solutions, all necessary equipment is located on the customer’s premises. This includes servers, storage and network equipment. The customer owns all equipment and is responsible for its maintenance.

  One of the main advantages of on-premise solutions is that there are clear dividing lines (Anderson, 2021). Everything within the customer’s building is their responsibility, while connections between offices are the responsibility of the network service provider.

  However, on-premise solutions also have some drawbacks. The equipment is considered a capital expenditure (CapEx), meaning the upfront cost is high (Anderson, 2021). New equipment can also take more than a week to install and will eventually require a technology update. Last, companies also need to consider redundancy to ensure that the service remains available in case of hardware failure.
- **Colocation (Colo) Services:** These services involve the use of a data centre facility owned by a third party and leased to external customers (Anderson, 2021). Customers retain ownership of their own equipment within the colofacility, but the facility owner is responsible for providing

highly available power, cooling and physical security according to the terms of the Service Level Agreement. Connections between customer offices and the colofacility are the responsibility of the network service provider.

As with on-site solutions, colo services incur CapEx costs for the customer's equipment within the facility. However, monthly hosting costs for the colo facility are considered operational costs (OpEx), which can be more easily managed on a monthly basis.

Installing new equipment in a colofacility can also take more than a week, and the equipment will eventually need a technology update. However, the facility owner is responsible for power and cooling, so the customer does not have to consider redundancy for those aspects. However, the customer is still responsible for the redundancy of the hardware it owns within the facility.

- **Server Virtualization:** This is a technology that allows multiple operating systems and applications to run on a single physical server (Anderson, 2021). This enables resource pooling, where multiple clients can share underlying hardware resources, see figure 3.1.

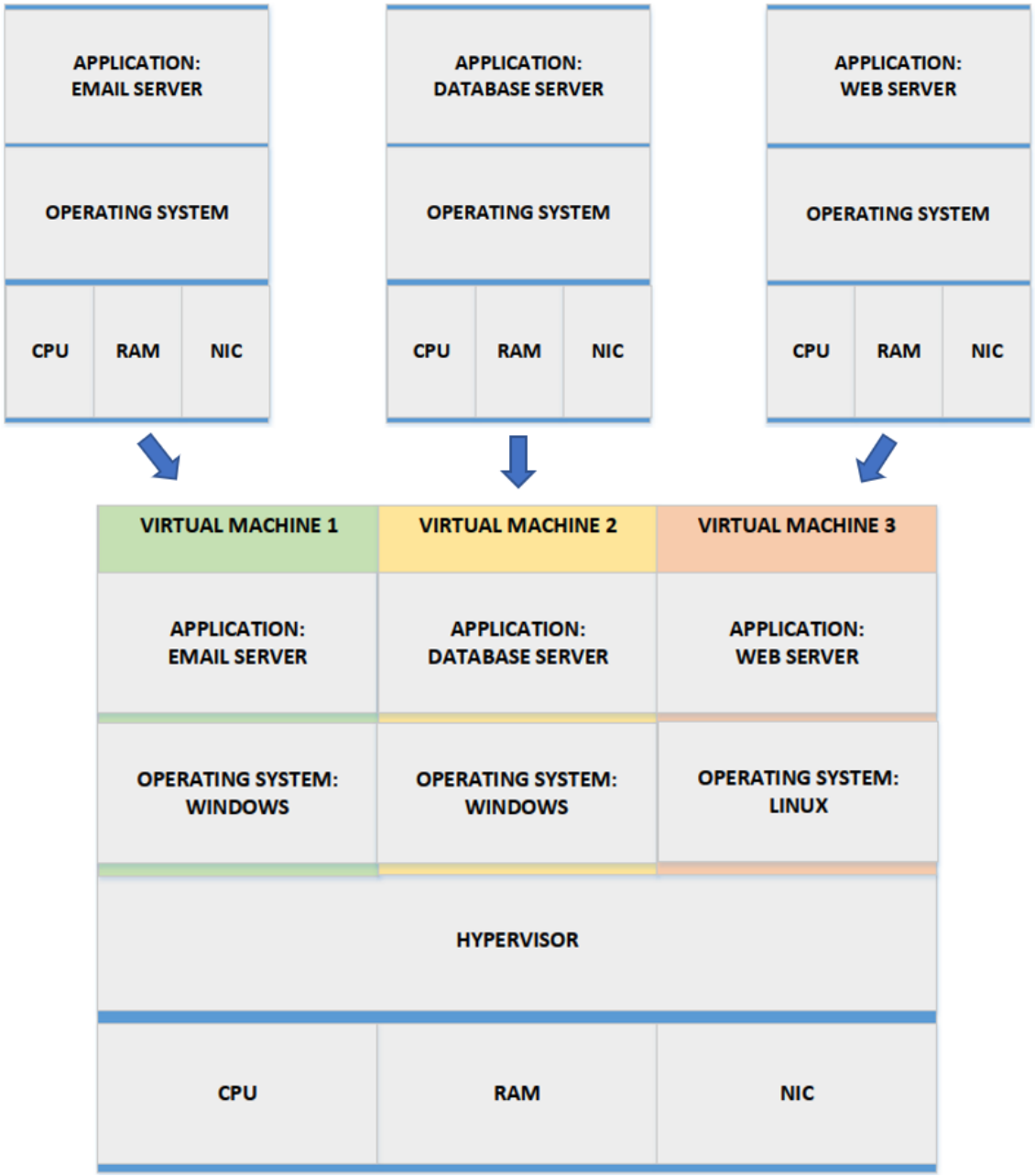

Figure 3.1: Server virtualization (Anderson, 2021)

Server virtualisation has been around for a long time and is considered the foundation of cloud computing. It allows companies to use their hardware resources more efficiently and reduce the cost of their IT infrastructure (Anderson, 2021).

However, it is important to mention that server virtualisation is not the same as cloud computing. While virtualisation enables resource sharing and can be used to offer cloud services, it does not provide the same benefits and features as a true cloud environment. This is because cloud computing uses shared infrastructure on demand that is managed and maintained by a third party, while server virtualisation uses dedicated hardware owned and maintained by the customer.

Cloud Computing

Cloud computing is a term often misunderstood. Some describe it as simply IT services located ”somewhere else”, but this is not quite correct. Colocation facilities, for example, are off premises but are not considered part of the cloud. Private clouds, on the other hand, are often located on premises. For a better understanding of cloud computing, it is important to consult the standard definition provided by the National Institute of Standards and Technology (NIST) (Mell and Grance, 2011):

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

According to NIST’s definition, cloud computing has several characteristics:

- **On-Demand Self-Service:** This allows consumers to unilaterally provision computing resources such as server time and network storage as needed, automatically and without human interaction with a service provider. This is a significant advantage over traditional on-premises or co-location deployments, where it can take at least a week to deploy a new workload due to the need for purchase approvals, server orders, physical installation and configuration by different teams.
- **Rapid Elasticity:** This allows servers to be rapidly provisioned and decommissioned based on current demand. This enables customers to save costs and is often a key justification for adopting cloud computing.
- **Broad network access:** This means that cloud capabilities are available over the network and accessible through standard mechanisms, making them easy to use on a variety of client platforms such as mobile phones, tablets, laptops and workstations.
- **Resource pooling:** The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model. This means that physical and virtual resources are dynamically allocated and reallocated based on consumer demand, and the customer typically has no control over or knowledge of the exact location of these resources, but can specify the location at a higher level of abstraction. Examples of resources that can be aggregated include storage, processing, memory and network bandwidth.
- **Measured Service:** This allows the use of resources to be automatically monitored and optimised through measurement at an appropriate level of abstraction. This allows resource usage to be monitored, controlled and reported, providing transparency for both the provider and the service user. Billing for cloud services is usually done on a monthly basis and is considered an operational expense from the customer’s point of view. Customers can choose between pay-as-you-go or fixed monthly plans, and the specific billing details depend on the service model used (IaaS, PaaS or SaaS).

Pros and cons of cloud computing

Cloud Computing offers companies a range of benefits (Anderson, 2021):

- **Scalability:** It allows companies to easily adapt their service level to their current needs. This means that companies can increase or decrease capacity as needed and access infinite computing capacity on demand by using cloud bursting.

- **Business agility:** This is enhanced by cloud computing, as it allows companies to quickly deal with expected or unexpected changes in load and reduces the time needed to put an application into production.
- **Cost efficiency:**This is another benefit of cloud computing, as customers only pay for what they need, resulting in directly proportional costs. This means customers do not have to make fixed provision for peak usage and can move from large initial CapEx costs to smaller monthly OpEx costs. ICT costs are also more transparent to the business, and the customer has no depreciable hardware assets. Technology renewal is the Cloud Provider's responsibility, and the provider passes on hardware maintenance costs to the customer as part of a predictable monthly fee, with no unexpected costs.
- **Competitive advantage:** It enables organisations to respond quickly to changing market trends and focus on growing their core business, while also freeing up resources to invest in innovation or other priority areas by reducing the capital spent on infrastructure.
- **Productivity:**This is increased by Cloud Computing, as IT staff can focus more on strategic decisions and developing and improving core applications instead of maintaining or troubleshooting internal ICT.
- **Availability and reliability:** All the Cloud Provider's key facilities are located in hardened data centres with redundant power supply, no single points of failure and on-site security. The service is also certified to relevant industry standards such as ISO 9001 (quality) and 27001 (security), and the data centre is built by qualified specialists according to best practices. It is important to check the Service Level Agreement to see what is guaranteed and what the compensation is if the SLA is not met.
- **Long-term cost:** The TCO of maintaining an On Premises solution should be compared with the TCO of maintaining a Cloud equivalent, and the pros and cons of both should be factored into the final decision. It is worth noting that most companies using cloud services have a mix of on-premises and cloud solutions.

However, besides advantages of cloud computing, there are also some disadvantages (Spiteri, 2020):

- **Downtime:** Cloud service providers claim to be available online 99.99% of the time, but even the most reliable services can have downtime or be unavailable for maintenance. Moreover, cloud services rely heavily on internet connectivity, which can be slow or erratic in certain locations and cause reduced productivity. Service failures can also result from factors beyond the cloud service provider's control, such as natural disasters or power outages, which can lead to significant downtime and business interruptions.
- **Security & Privacy:** The use of cloud services can have security risks, as sensitive data may be vulnerable to cyberattacks and breaches. Cloud service providers may have more resources and be more secure than in-house storage, but there are still potential risks. Businesses should carefully consider the type of information they store in the cloud and be aware of regulatory compliance concerns, particularly in regulated industries like healthcare and finance. Data loss due to technical problems or human error is also a risk that can cause significant disruption to businesses.
- **Control:** Cloud providers offer managed services, which can be beneficial for non-tech-savvy users as everything is taken care of for them. However, users have limited control and customizability over the infrastructure and technology, which can be frustrating for those who prefer full control over their IT environment. Cloud services may not offer the same level of customization as on-premises solutions, which can be problematic for businesses with specific needs. Additionally, cloud services can restrict access to data, making it difficult for companies to gain insights and develop their own analytics solutions, particularly for companies with unique data analytics needs.
- **Potential vendor lock-in:** This may not be a problem at first, but it is important to keep in mind that it can be difficult to switch cloud service providers because they often use proprietary technologies and data formats, which can lead to vendor lock-in. However, once you have been using a cloud service for a while, you may find it easier to switch providers. This is especially relevant if you are using a small provider that you may outgrow in a few years.

Cloud Service Models

The National Institute of Standards and Technology (NIST) defines three service models for how cloud services can be offered (Mell and Grance, 2011). See figure 3.2 for a full overview of the different service models.

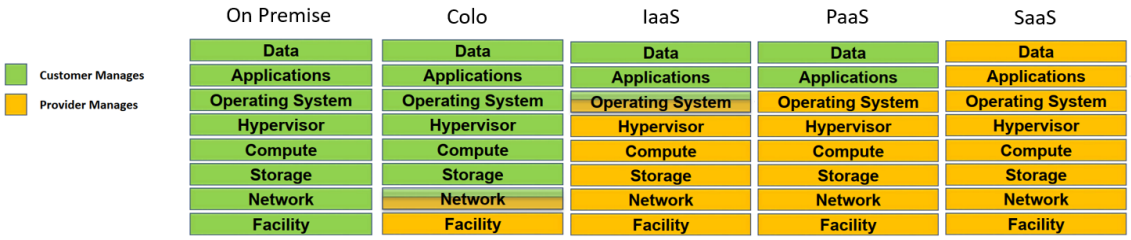

Figure 3.2: Service models

As can be seen in table 3.2, the different cloud service models differ from each other in a number of areas. Below they are explained individually:

- **Infrastructure as a Service (IaaS):** Infrastructure as a Service (IaaS) is a type of cloud computing service that allows consumers to provide and use basic computing resources, such as processing, storage and networking, without managing or controlling the underlying infrastructure. Consumers have control over operating systems, storage and applications used, and may have limited control over certain network components, such as host firewalls.
- **Platform as a Service (PaaS):** PaaS, or Platform as a Service, refers to the ability for consumers to deploy their own applications on a cloud infrastructure (Anderson, 2021). The underlying cloud infrastructure, including servers, operating systems and storage, is managed by the provider, but the consumer has control over the deployed applications and possibly the configuration settings for the environment in which the applications are hosted. Some examples of PaaS include AWS Elastic Beanstalk, Microsoft Azure, Google Apps, Salesforce Force.com and IBM Bluemix. PaaS is usually billed based on memory usage.
- **Software as a Service (SaaS):** SaaS, or Software as a Service, refers to the ability of consumers to outsource almost all services to the Cloud provider (Anderson, 2021). In this model, the provider provides access to software applications over the internet. The provider is responsible for managing the infrastructure, operating system and software applications, while the customer is only responsible for accessing and using the software (Anderson, 2021).
- **Anything as a Sevice (XaaS):** In addition to PaaS and SaaS, many cloud providers also offer other ”as a Service” offerings, sometimes referred to as XaaS or ”Anything as a Service” (Anderson, 2021). Examples include BaaS or Backup as a Service, DRaaS or Disaster Recovery as a Service, DaaS or Desktop as a Service, and Storage as a Service such as Amazon S3, Google Drive, Microsoft OneDrive and Dropbox.

Large cloud server providers often offer multiple models, allowing customers to choose the level of responsibility and access that best suits their needs. The three models build on each other, with IaaS offering the lowest level of access and responsibility and SaaS the highest. The choice of model depends on customers' specific needs and their level of expertise in managing cloud infrastructure.

Cloud Deployement models

Cloud deployment models refer to the way cloud computing resources are provided to users. The National Institute of Standards and Technology (NIST) distinguishes four main deployment models: Public, Private, Community and Hybrid (Mell and Grance, 2011).

- **Public:** These clouds are open to the general public and are owned, managed and operated by a business, academic or government organisation. Examples of public cloud providers include Amazon Web Services, Microsoft Azure, IBM Bluemix and Salesforce. This is the most common deployment model.

- **Private:** These clouds, on the other hand, are for the exclusive use of one organisation and its multiple users. They may be owned, managed and operated by the organisation itself, a third party or a combination of both, and may be located on or off premises. Private clouds meet the essential characteristics of cloud computing, including on-demand self-service, fast elasticity, wide network access, resource pooling and measured service. They are best suited to large enterprises looking to increase efficiency and ROI over the long term.
- **Community:** These clouds are for the exclusive use of a specific community of consumers with shared interests, such as mission, security requirements, policies and compliance considerations. They may be owned, managed and operated by one or more community organisations, a third party or a combination of both, and may be located on or off-site.
- **Hybrid:** These clouds are a combination of two or more separate cloud infrastructures that remain unique entities but are connected by technology that enables portability of data and applications. Companies can use hybrid clouds to house their cloud in public clouds for additional capacity or to use public clouds for disaster recovery. Hybrid clouds are less common than the other deployment models.

3.1.2. Current state of the market

This section first provides a brief market analysis and then discusses the three most popular cloud platforms (AWS, Azure and Google).

Market analysis

The financial industry is rapidly adopting cloud platform services due to the numerous benefits they provide, including increased efficiency, scalability, and cost savings (MarketsandMarkets, 2020). According to a report by FMI (FMI, 2021), the global cloud platform market in the financial sector is projected to experience significant growth in the next few years, with a compound annual growth rate of 12.4% and a projected increase from $23.7 billion in 2022 to $90.1 billion by 2032.

There are several major players in the cloud platform market in the global financial sector, with AWS, Azure and Google the leaders (See figure 3.3). Amazon Web Services (AWS) is a leading provider, offering a range of services specifically designed for the financial industry, including the ability to process large amounts of data for risk analysis and compliance purposes. AWS also has a strong track record of security and compliance, which is essential for financial institutions. Microsoft Azure is another prominent provider, offering solutions for banking, insurance, and capital markets. Google Cloud is also a significant player in the financial sector, with a focus on artificial intelligence and machine learning capabilities.

Figure 3.3: Cloud Infrastructure and Platform Services Leaders 2022 (Mitford, 2022)

In the Netherlands, the adoption of cloud platforms in the financial sector has seen significant growth in recent years (Brits et al., 2021). Many financial institutions, including banks and insurance companies, have recognized the benefits of using cloud platforms, including cost savings, increased efficiency, and enhanced security. There are several major providers of cloud platform services in the Dutch financial sector, including AWS, Microsoft Azure, and Google Cloud. These providers offer a range of services, including infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). AWS has a strong presence in the Dutch financial sector, with a market share of around 40%. Microsoft Azure is also popular in the Netherlands, with similar market shares. While Google Cloud has a more limited presence in the Dutch financial sector, with a market share of around 15%, see results in appendix A.1. In addition to these major players, there are also several smaller, local providers offering cloud platform services in the Dutch financial sector, including IBM and Oracle, completing the last 5% of market share. These providers may offer specialized services tailored to the specific needs of the Dutch financial market.

Overall, the demand for cloud platform services in the financial sector is expected to continue to grow in the coming years. Financial institutions are increasingly recognizing the benefits of using cloud platforms and are seeking ways to leverage these technologies to improve efficiency, reduce costs, and enhance security.

Cloud Computing platforms

Cloud computing platforms offer computing services through the internet and allow users to access and use these services on a pay-as-you-go basis without investing in infrastructure upfront. There are three types of cloud computing platforms: IaaS, PaaS, and SaaS. Some popular cloud platform providers among financial institutions include Amazon Web Services, Microsoft Azure, and Google Cloud. Other cloud platforms in the financial sector include Salesforce, Oracle Cloud, and IBM Cloud.

In this section, the three most popular Cloud platforms will be briefly discussed.

- **Amazon Web Services (AWS)** Cloud computing has revolutionized the way we access and use computing resources. Amazon Web Services (AWS), launched by Amazon in 2002, is one of the leading cloud computing platforms in the market (Maarek, n.d.). It was made available to the public in 2004 with the introduction of its first offering, Simple Queue Service (SQS). Since then, AWS has continuously expanded its offerings and global presence, with annual revenue of $35 billion and a 47% market share in the cloud computing industry, according to the Gartner magic quadrant.

  AWS has a vast global network consisting of regions, availability zones, data centers, edge locations, and points of presence. Its regions are connected by a private network, and within each region are availability zones, which are physically separate locations equipped with redundant power, networking, and cooling.

  AWS's infrastructure is divided into three main layers: platform services, foundation services, and infrastructure. Platform services cover a wide range of domains, including databases, analytics, app services, management tools, developer tools, mobile services, and the Internet of Things. Foundation services are further divided into five categories: compute, network, storage, security and identity, and applications.
- **Microsoft Azure:** Microsoft Azure is a cloud computing platform and infrastructure created by Microsoft for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers (Mitchell, n.d.). It provides a range of cloud services, including those for computing, analytics, storage, and networking. Users can choose and configure these services to meet their specific needs.

  Azure was first released in 2010 and has since become one of the leading cloud computing platforms in the market. It is used by a variety of businesses and organizations worldwide, from small startups to large enterprises. Azure supports a number of programming languages, tools, and frameworks, making it a versatile platform for a wide range of applications.

  In addition to its various cloud services, Azure also offers tools and services for integrating on-premises IT environments with the cloud, as well as data analytics and machine learning capabilities. It also provides a range of security features, such as identity and access management, data protection, and threat protection.

  Overall, Microsoft Azure is a comprehensive cloud computing platform that offers a wide range of services and tools for building, deploying, and managing applications and services in the cloud.
- **Google Cloud Platform (GCP):** Google Cloud Platform (GCP) is a large, global cloud infrastructure provider with a significant presence on multiple continents. It has a customer base in over 200 countries, and its infrastructure consists of 20 regions and 61 zones (Janakiram, n.d.).

  Google Cloud Platform has over 100 services spanning infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). It offers a wide range of services beyond the key building blocks of compute, storage, and network. These additional services include databases, data and analytics, machine learning, API management, hybrid and multi-cloud capabilities, and workload migration. It also has security and DevOps services that cover the entire stack, as well as management tools for customers to manage their deployments and infrastructure.

  The services offered by GCP are organized into several categories:

  - Compute: This category includes various services such as infrastructure as a service, App Engine, containers, functions as a service, and a container registry.
  - Storage and database: This category includes object storage, block storage, and various databases such as NoSQL, RDBMS, and in-memory databases.
  - Network: This category includes services such as Cloud Virtual Network, load balancing, CDN, and hybrid capabilities.
  - Security: This category includes services like Cloud IAM, Cloud Security Scanner, and Platform Security.
  - AI and machine learning: This category includes services such as ML Engine and APIs.
  - DevOps: This category includes tools such as Cloud SDK and Deployment Manager.
  - Management tools: This category includes services like Stat Driver and APIs.

In addition to these services, GCP also offers additional services such as API analytics, IOT Core, VPN, and AutoML, which are relevant to various areas such as AI and machine learning, migration, multi-cloud, and API management.

3.2. Policy arena

This section dives into the policy arena surrounding cloud adoption in the Dutch financial sector. In the first section, the different IT and cloud regulations that affect cloud adoption in this sector are discussed. The second part discusses what European guidelines are in place to guide financial institutions on their journey to the cloud. Finally, a conclusion is formulated by summarising the previous sections and show how they lead to specific requirements for cloud adoption in the Dutch financial sector.

3.2.1. Regulations and impact on Cloud adoption

In this section, the most important IT regulations related to cloud in the Dutch financial sector are discussed. A complete overview of all regulations can be seen in the table 3.1.

Table 3.1: Cloud adoption regulations

Name	Explanation	Impact on Cloud Adoption
GDPR	Policy to protect personal data of EU citizens. It obliges companies within the EU and those based outside processing EU citizens' data.	It requires financial institutions to take precautionary measures to protect personal data and comply with all regulations, which can be achieved through the use of secure and compliant cloud services.
PSD2	EU directive that aims to improve consumer protection and security, as well as boost innovation and competition in the payment services market. It requires financial institutions to implement strong customer authentication and secure communication methods.	It is expected to boost the adoption of cloud services in the financial sector as they can aid in scalability and efficiency while providing new opportunities for innovation and competition. Additionally, cloud services can help financial institutions meet the directive's robust security requirements to protect customer data.
MiFID	A directive created by the EU to increase integrity and transparency in financial markets. It requires financial institutions to maintain accurate and complete records of their trading activities and ensure the security and resilience of their IT systems.	This directive requires that financial institutions meet specific requirements for data storage and processing.
NISD	A directive created by the European Union to improve the resilience and security of network and information systems (NIS).	Financial institutions covered by critical infrastructure must take measures to protect against cyber-attacks, including additional security requirements for cloud service providers.
Cyber Act	Laws put in place by the European Union to ensure the security and resilience of digital services and infrastructure in the EU.	Financial institutions must ensure that their cloud providers comply with EU cybersecurity regulations and undergo a certification process. Due diligence on the cyber security of cloud providers is required. Cloud providers must also demonstrate compliance with EU cybersecurity regulations.
AMLD	A set of rules to prevent money laundering and terrorist financing in the European Union.	Compliance with AMLD's data protection and retention requirements can be difficult with cloud platforms. Specialized cloud providers that offer enhanced security measures, data sovereignty features, and detailed monitoring and reporting capabilities can help financial institutions comply with the guidelines.
Wft	Dutch law regulating the financial sector, including the use of technology, in the Netherlands.	Shapes the adoption of Cloud platforms in the financial sector in the Netherlands by requiring financial institutions to comply with strict data security and privacy regulations.
Wwft	Dutch law aimed at preventing money laundering and terrorist financing by imposing strict rules on financial institutions and other regulated entities.	Affects the adoption of cloud platforms in the financial sector, as financial institutions must ensure that their cloud providers have the necessary security measures in place to protect sensitive financial data.
ISO/IEC 27000 standards	International standards for information security management which provides a framework for protecting sensitive information like financial data.	Helps organizations to ensure their cloud platforms comply with it to mitigate the risks associated with data breaches and other security incidents.
PCI DSS	This is a set of guidelines and standards designed to protect cardholder data and prevent fraud. It applies to any organization that processes, stores, or transmits credit card information, including financial institutions	Institutions must ensure that all data is encrypted and protected, implement strict access controls and regularly monitor and audit their systems. Cloud providers that cater to the financial sector must be able to meet these requirements and demonstrate their compliance with the PCI DSS, which can slow down the adoption process.
DORA	This is a proposed EU law that aims to enhance the resilience and security of digital infrastructure used by financial institutions	It will likely lead to increased scrutiny of cloud providers and their security practices by financial institutions. It may also result in increased costs for financial institutions as they work to meet these new requirements. Cloud providers will need to be able to demonstrate their ability to prevent, detect, and respond to cyber threats and operational disruptions to remain compliant with the DORA, which could impact their adoption.

The sections below briefly discuss what the regulations exactly entail and how it affects cloud adoption within this sector.

General Data Protection Regulation (GDPR)

This is a regulation introduced by the European Union (EU) in 2018 to protect personal data of EU citizens (Official Journal of the European union, 2016). It affects all companies within the EU and those based outside the EU but processing EU citizens' data. For companies in the Dutch financial sector, it affects the adoption of cloud platforms, as it obliges them to ensure that their cloud provider complies with the requirements for storing and processing personal data. This means taking appropriate security measures to protect personal data and being able to complete requests for access and deletion of data within a significant time. In addition, they are also required to appoint a data protection officer (DPO) who is responsible for GDPR compliance and can notify authorities within 72 hours in case of possible data breaches. All in all, this regulation has a significant impact on cloud adoption within this sector, as it requires financial institutions to take precautionary measures to protect personal data and comply with all regulations.

Payment Services Directive 2 (PSD2)

This is a European Union directive that aims to improve consumer protection and security, as well as boost innovation and competition in the payment services market (Official Journal of the European Union, 2015). One of the key aspects of this directive is that financial institutions are required to implement strong customer authentication and secure communication methods for online payment services to prevent potential fraud and unauthorized access to payment accounts. Additionally, financial institutions will be required to open their systems to third parties, known as Payment Service Providers (PSPs), to access customer account information and initiate payments on their behalf. This could lead to an increase in the adoption of cloud services in the financial sector as they can aid in scalability and efficiency while providing new opportunities for innovation and competition. Furthermore, PSD2 also requires financial institutions to take robust security measures to protect customer data, which is easier to achieve with cloud services. Overall, PSD2 is expected to boost the adoption of cloud services in the financial sector.

Markets in Financial Instruments Directive (MiFID II)

This is a directive created by the European Union to increase integrity and transparency in financial markets (Official Journal of the European Union, 2014). It aims to protect investors and reduce the risk of market abuse by introducing controls and robust IT systems for investment firms. The regulation entered into force in 2018 and requires financial institutions to maintain accurate and complete records of their trading activities and ensure the security and resilience of their IT systems. This may pose challenges to the adoption of cloud services as they need to ensure compliance before using them. Despite these challenges, many financial institutions have implemented cloud platforms for data storage and analytics to comply with MiFID II requirements as they provide necessary security, scalability, and compliance capabilities. However, the use of cloud platforms in the financial sector is still restricted by regulations such as MiFID II, which requires that they meet specific requirements for data storage and processing. Financial institutions must ensure that these platforms meet these requirements.

Network and Information Systems Directive (NISD)

This is a directive created by the European Union in 2016 to improve the resilience and security of network and information systems (NIS) and requires organisations covered by critical infrastructure to take measures to protect against cyber-attacks (Official Journal of the European Union, 2016). Financial institutions must ensure compliance with NISD requirements, including incident management processes and cyber incident reporting, and additional security requirements for cloud service providers. These requirements can make it more difficult for companies in the financial sector to use cloud platforms, but there are frameworks such as those provided by NDO that can help them choose a secure provider.

EU Cybersecurity Act and Certification Framework

The EU Cybersecurity Act and the EU Cybersecurity Certification Framework are laws put in place by the European Union to ensure the security and resilience of digital services and infrastructure in the EU (Official Journal of the European Union, 2019). They have a significant impact on the adoption of cloud

platforms in the financial sector, as they require financial institutions to ensure that the cloud platforms, they use comply with EU cybersecurity regulations. For instance, they must conduct due diligence on the cyber security of their cloud providers and ensure that their cloud providers comply with EU cybersecurity standards. In addition, cloud providers must also demonstrate that their products, services, and processes comply with EU cybersecurity regulations by undergoing a certification process.

EU Anti-Money Laundering Directive (AMLD)
This is a set of rules to prevent money laundering and terrorist financing in the European Union (Official Journal of the European Union, 2018). It requires financial institutions and other businesses to take robust measures to identify and verify customers and monitor and report suspicious transactions. Cloud platforms can make it difficult to comply with the AMLD's data protection and retention requirements. However, financial institutions can engage specialised cloud providers that offer enhanced security measures, data sovereignty features and detailed monitoring and reporting capabilities to comply with the guidelines. By taking advantage of this, financial institutions can achieve cost efficiency, scalability and flexibility, while ensuring compliance with the AMLD.

Financial Supervision Act (Wft)
This is a Dutch law regulating the financial sector, including the use of technology, in the Netherlands (Koninkrijksrelaties, n.d.-a). The law sets strict requirements on data security, data privacy and data management those financial institutions, including banks, insurance companies and investment firms, operating in the Netherlands must comply with. As such, the Wft plays an important role in shaping the adoption of Cloud platforms in the financial sector in the Netherlands by requiring financial institutions to comply with strict data security and privacy regulations.

Anti-Money Laundering and Counter-Terrorism Financing Act (Wwft)
This is a Dutch law aimed at preventing money laundering and terrorist financing by imposing strict rules on financial institutions and other regulated entities (Koninkrijksrelaties, n.d.-b). This affects the adoption of cloud platforms in the financial sector, as financial institutions must ensure that their cloud providers have the necessary security measures in place to protect sensitive financial data, perform due diligence on their cloud providers and ensure proper access controls to prevent unauthorised access. This places a significant burden on financial institutions and their cloud providers, making it more difficult to adopt cloud platforms, but with the right security measures in place, financial institutions can still benefit from cloud computing while complying with the Wwft.

ISO/IEC 27000 standards (Information security management)
These are international standards for information security management which provides a framework for protecting sensitive information like financial data by implementing policies, procedures and risk management, access control and incident management (ISO, n.d.). In the financial sector, the adoption of cloud platforms is becoming increasingly popular, however it poses a significant risk to the security of financial data. ISO 27001 helps organizations to ensure their cloud platforms comply with it to mitigate the risks associated with data breaches and other security incidents. Additionally, it helps organizations to meet regulatory requirements such as PCI DSS and GDPR.

Payment Card Industry Data Security Standard (PCI DSS)
This is a set of guidelines and standards that are designed to protect cardholder data and prevent fraud. It applies to any organization that processes, stores, or transmits credit card information, including financial institutions (Baykara, 2020). In the financial sector, the PCI DSS has a significant impact on the adoption of Cloud platforms, as institutions must ensure that all data is encrypted and protected, implement strict access controls and regularly monitor and audit their systems. Cloud providers that cater to the financial sector must be able to meet these requirements and demonstrate their compliance with the PCI DSS, which can slow down the adoption process.

Digital Operational Resilience Act (DORA)
This is a proposed EU law that aims to enhance the resilience and security of digital infrastructure used by financial institutions (European Commission, 2020). It will require these organizations to have in place robust plans and processes to prevent, detect, and respond to cyber threats and operational

disruptions. This will likely lead to increased scrutiny of cloud providers and their security practices and may also result in increased costs for financial institutions as they work to meet these new requirements. (Carrier, 2020).

3.2.2. Guidelines for Cloud adoption

The European Securities and Markets Authority (ESMA) has published guidelines for firms that outsource their operations to cloud service providers (CSPs) to ensure compliance and security (ESMA, 2021). These guidelines should ensure consistent, efficient and effective supervisory practices within the European financial system. This allows financial institutions to outsource to the cloud in a common, uniform and consistent manner. In particular, they help identify and address risks and challenges arising from cloud outsourcing arrangements, from the decision to outsource, the selection of a cloud service provider, the monitoring of outsourced activities to the definition of exit strategies.

The guidelines include the following key points:

1. **Governance, oversight, and documentation:** Firms should have a clear strategy for managing and controlling cloud outsourcing, assign responsibilities, allocate resources for compliance, establish an oversight function, and monitor performance and security measures of CSPs. They should also reassess critical or important functions periodically and maintain a register of all cloud outsourcing arrangements.
2. **Pre-outsourcing analysis and due diligence:** Before outsourcing, firms must assess if the arrangement concerns a critical or important function, identify, and assess relevant risks, undertake appropriate due diligence on the prospective CSP, and identify and assess any conflict of interest that the outsourcing may cause.
3. **Key contractual elements:** The contract should clearly outline the rights and obligations of the firm and CSP, the possibility for termination, and specific details such as the outsourced function, start and end dates, financial obligations, sub-outsourcing, location and data processing, information security and personal data protection, monitoring and performance targets, reporting obligations, incident management, insurance, business continuity and disaster recovery plans, and access and audit rights for the firm, competent authorities, and any other appointed parties.
4. **Information Security:** Firms should set information security requirements in internal policies and procedures, as well as in the cloud outsourcing agreement, and monitor compliance on an ongoing basis. For critical or important functions, a risk-based approach should be used, including clear allocation of information security roles and responsibilities between the firm and CSP, strong authentication mechanisms and access controls, encryption and key management, appropriate network security, secure API integration, effective business continuity and disaster recovery controls, risk-based data storage and processing locations, and compliance and monitoring of the CSP's information security standards.
5. **Exit Strategies:** Firms should be able to exit the cloud outsourcing arrangement without disruption to their business activities or compliance with regulations and without compromising the confidentiality, integrity, and availability of their data. To achieve this, firms should develop comprehensive, documented, and tested exit plans, identify alternative solutions, and develop transition plans, and ensure that the cloud outsourcing agreement includes an obligation for the CSP to support the orderly transfer of data and functions.
6. **Access and Audit Rights:** The European Securities and Markets Authority (ESMA) has provided guidelines on outsourcing to cloud service providers. These guidelines state that firms should ensure that the written agreement with the cloud service provider (CSP) does not limit their access and audit rights and oversight options on the CSP. The frequency and areas of auditing should be determined based on the importance and risk of the outsourcing arrangement. The CSP should provide a clear rationale if the exercise of access or audit rights creates a risk for the environment and agree on alternative ways to achieve a similar result. Firms may also use third-party certifications and reports, as well as pooled audits with other clients of the same CSP. However, for outsourcing of critical or important functions, firms should assess the adequacy and sufficiency of these certifications and reports and thoroughly assess and verify them on a regular basis. They should also retain the right to perform individual on-site audits at their discretion. Prior notice should be given to the CSP before an on-site visit unless it is not possible due to an emergency or critical situation.

7. **Sub-outsourcing:** The European Securities and Markets Authority (ESMA) has provided guidelines on outsourcing to cloud service providers (CSPs) regarding sub-outsourcing. If sub-outsourcing of critical or important functions is permitted, the written agreement between the firm and the CSP should specify which parts of the outsourced function are excluded from potential sub-outsourcing, indicate the conditions to be complied with in case of sub-outsourcing, and specify that the CSP remains accountable and is obliged to oversee the services that it has sub-outsourced. The agreement should also include an obligation for the CSP to notify the firm of any intended sub-outsourcing or material changes, and the firm should have the right to object or require explicit approval before the proposed sub-outsourcing or changes take effect. The firm should also have the right to terminate the cloud outsourcing arrangement in case of undue sub-outsourcing. The firm should also ensure that the CSP appropriately oversees the sub-outsourcer.
8. **Written notification to competent authorities:** The European Securities and Markets Authority (ESMA) has issued a guideline on outsourcing to cloud service providers, stating that firms should notify their competent authority in writing and in a timely manner of planned cloud outsourcing arrangements that concern a critical or important function. The notification should include information such as the start and end date of the agreement, the outsourced function, the reasons for its classification as critical or important, and information about the cloud service provider. The firm should also notify the authority of any changes in the classification of a function from non-critical to critical or important. The notification should also include information about the governing law and jurisdiction, deployment models, data storage locations, and any sub-outsourcers involved.
9. **Supervision of cloud outsourcing arrangements:** The European Securities and Markets Authority (ESMA) has issued a guideline on the supervision of cloud outsourcing arrangements, which states that competent authorities should assess the risks arising from firms' cloud outsourcing arrangements as part of their supervisory process. This assessment should focus on the arrangements that relate to the outsourcing of critical or important functions, and authorities should be satisfied that they are able to perform effective supervision, particularly when firms outsource critical or important functions that are performed outside the EU. The guideline also states that authorities should assess on a risk-based approach whether firms have the necessary governance, resources, and operational processes in place to enter, implement, and oversee cloud outsourcing arrangements, and whether they identify and manage all relevant risks related to cloud outsourcing appropriately and effectively. If concentration risks are identified, authorities should monitor the development of such risks and evaluate both their potential impact on other firms they supervise and the stability of the financial market.

3.3. Conclusion

Finally, based on the technology description, we can conclude that AWS, Azure and Google Cloud Platform are currently the largest players in the Cloud platform market. Therefore, only these three are included in this study

Furthermore, based on the policy arena, a conclusion is made that based on the regulations and guidelines regarding Cloud in the Dutch financial sector, the various Cloud platforms should be carefully considered if a financial institution is considering switching to a Cloud Provider. The guidelines state that financial institutions should take several steps if they want to outsource via a platform provider. It is therefore advised to test the different platforms in several areas.

The following chapters examine which factors are very important when choosing a cloud platform in this sector. Also, the three most popular platforms are eventually ranked on these factors, ultimately revealing which platform is the most suitable for this sector.

4

Factors

This chapter discusses the categories and associated factors that are eventually included in further analyses. As discussed in chapter 2, van der Kaa's framework (van de Kaa et al., 2011) is used as the basis for the factors. A literature review and exploratory interviews were conducted to examine which of these 29 factors are relevant and are included in further analyses. We also examined which specific Cloud factors could potentially be added to this framework. This ultimately resulted in a set of five categories with a total of 29 factors relevant for the adoption of a Cloud Platform within the Dutch financial sector. These categories and factors are detailed last.

4.1. Selection of relevant factors

This section uses a literature review and the first round of interviews to identify which factors from van der Kaa's framework are relevant to the Cloud Platform battle. It also looked at specific cloud factors that could potentially be added to the framework.

A total of 26 articles were reviewed and three interview were conducted to identify the relevant factors for this topic, see appendix B. The articles all focused on cloud (platforms) adoption, but individually had slightly different approaches. For each article, we looked at whether a particular factor was addressed and for each interview, the experts were asked if they thought the factor is relevant. Ultimately, this resulted in a counting of the factors in the interviews and articles, see the table below.

Table 4.1: Factor count in literature

#	Factors	Mentions in interviews	Mentions in literature	Total (#)	Total (%)
Firm level factors					
Characteristics of the format supporter					
1	Financial strength	3	6	9	31,0
2	Brand reputation and credibility	3	6	9	31,0
3	Operational supremacy	3	7	10	34,5
4	Learning orientation	3	6	9	31,0
5	Location of data	0	4	4	13,8
6	Customer support	0	1	1	3,5
Characteristics of the format					
7	Technological superiority	3	14	17	58,6
8	Compatibility	3	12	15	51,7
9	Complementary goods	2	1	3	10,3
10	Flexibility	3	4	7	24,1
11	Scalability	0	7	7	24,1
12	Complexity	0	8	8	27,6
13	Security & Privacy	0	21	21	72,4
14	Availability	0	10	10	34,5
15	Trialability	0	2	2	6,9
16	Recovery	0	2	2	6,9
17	Implementation times	0	2	2	6,9
Format support strategy					
18	Pricing strategy	3	20	23	79,3
19	Pre-emption of scarce assets	1	0	1	3,5
20	Appropriability strategy	1	0	1	3,5
21	Timing of entry	3	1	4	13,8
22	Marketing Communications	3	0	3	10,3
23	Distribution strategy	3	0	3	10,3
24	Commitment	3	7	10	34,5
Other stakeholders					
25	Current installed base	3	1	4	13,8
26	Previous installed base	1	0	1	3,5
27	Big Fish	2	1	3	10,3
28	Antitrust laws	2	0	2	6,9
29	Suppliers	2	1	3	10,3
30	Effectiveness of the format development process	2	0	2	6,9
31	Network of stakeholders	3	2	5	17,2
32	Regulator	2	16	18	62,1
Environmental factors					
Market characteristics					
33	Bandwagon effect	2	6	8	27,6
34	Network externalities	2	3	5	17,2
35	Number of options available	2	1	3	10,3
36	Uncertainty in the market	2	2	4	13,8
37	Rate of change	2	3	5	17,2
38	Switching costs	3	6	9	31,0
39	Cultural barriers	0	1	1	3,5

White Factors derived from van der Kaa's framework (van de Kaa et al., 2011).
Orange New added cloud specific factors.
Dark green Relevant factors for cloud platform adoption.
Red Irrelevant factors for cloud platform adoption.
Light green Firm level categories.
Yellow Environmental categories.

Table 4.1 shows that a total of 39 factors were found in the 26 articles and three interviews. In addition to the 29 factors from van de Kaa's framework (van de Kaa et al., 2011), 10 factors were found that also relate to the Cloud Platform battle. It was finally decided to include only the factors mentioned in more than 10% of the articles and interviews. This percentage was chosen because the factors mentioned in less than 10% of articles could be seen as irrelevant to cloud platform adoption. The factors mentioned less frequently have not been included. The following sections discuss the final factor list.

4.2. Categories

Eventually, a list of 29 factors emerged, all of which were relevant to this cloud platform battle, and it was decided to stick to comparable categories as in de Kaa's framework (van de Kaa et al., 2011), as all factors could be classified in those categories. However, the categories were renamed to be more in line with the topic of this paper. The factors were finally classified into the following categories: *Characteristics of the Cloud provider*, *Characteristics of the Cloud Platform*, *Cloud provider support strategy*, *Other stakeholders* and *Market characteristics*. Here, the *Market characteristics* category only includes *Environmental factors*, which can be seen as external factors that cannot be influenced by the Cloud Provider. All other categories contain *Firm Level factors*, which the Cloud provider can influence directly or indirectly. See all relevant factors and categories in the table below.

Table 4.2: Final list of factors

#	Factors	Definitions
Firm level factors		Impact on Cloud Platform dominance
Characteristics of the Cloud provider		
1	Financial strength	The current and future financial strength of the Cloud provider.
2	Brand reputation and credibility	Reputation of the cloud provider and its previous track record.
3	Operational supremacy	The Cloud provider's ability to exploit resources more effectively than the competition.
4	Location of data	The location of data centers and the potential impact on data privacy and security
5	Learning orientation	The core capabilities, know-how and absorptive capacity of the Cloud provider and ability utilize them.
Characteristics of the Cloud Platform		
6	Technological superiority	Platform design as having features that allow this design to outperform other traditional and competitor designs
7	Compatibility	The compatibility of the organization's existing systems and infrastructure with cloud services
8	Complementary goods	Substitute programs or products that together fulfill a common want
9	Flexibility	Incremental cost and time needed to adapt the platform due to new developments of the technology
10	Scalability	The ability to easily scale up or down the amount of resources used as needed
11	Complexity	The degree of platform complexity of using cloud services and their integration with existing systems
12	Security & Privacy	The degree of security and privacy of data stored in the cloud
13	Availability	The ability to get stable access to data and services from anywhere with an internet connection
Cloud provider support strategy		
14	Pricing strategy	Actions of strategic pricing taken by firm(s) to achieve market share in order to affect the dominance process.
15	Timing of entry	Point in time when a platform is introduced into the market.
16	Marketing Communications	All the actions to influence customer expectations.
17	Distribution strategy	Strategy which the firm(s) use to distribute the format to the market.
18	Commitment	The level of dedication and effort a company is willing to invest in promoting and supporting their platform.
Other stakeholders		
19	Current installed base	The current amount of particular cloud platforms implemented in companies.
20	Big Fish	Presence and actions of a large firm with a considerable influence in the industry.
21	Regulator	Presence of regulatory bodies and actions taken by them which influence the battle.
22	Suppliers	Suppliers of complementary goods.
23	Network of stakeholders	The attributes of the stakeholder network. This encompasses the size of the network, diversity and power of the network.
Environmental factors		External factors
Market characteristics		
24	Bandwagon effect	As other users adopt a particular Cloud platform, others will be inclined to follow as a result.
25	Network externalities	Network externalities refers to the increase in utility which occurs when more users adopt the same Cloud platform.
26	Number of options available	Number of options which can replace the Cloud platform.
27	Uncertainty in the market	Level of uncertainty in the market which affects the firm's commitment to support the Cloud platform.
28	Rate of change	The overall speed of change in technology, market and industry.
29	Switching costs	The costs incurred when switching from the current Cloud platform to another platform.

Green Firm level factors.
Yellow Environmental factors.

In the sections below, the factors and the associated factors are explained individually.

4.2.1. Characteristics of the Cloud Provider

The first category refers to the strength of the cloud provider's characteristics. Thus, we assume here that there are multiple providers offering cloud. The stronger the characteristics of the cloud provider, the more likely a cloud provider will become dominant. The factors within this category are discussed separately below:

- **Financial Strength:** The current and future financial strength of the Cloud provider. This has everything to do with the financial resources the provider has or will have in the future. If a provider scores well on this, they are more likely to be able to keep the cloud platform alive longer. They will also have more money to spend on marketing the platform (Schilling, 1999).
- **Brand reputation and credibility:** Reputation of the cloud provider and its past track record. Past experience has shown that this is an important factor in the success of a format (Axelrod et al., 1995). If a particular provider has a better track record than its competitor, it is more likely to be acquired.
- **Operational supremacy:** The Cloud provider's ability to exploit resources more effectively than its competitors. For example, this can be achieved by possessing a superior production capability (Agarwal et al., 2017). A technological advantage can make a Cloud Provider more likely to become dominant.
- **Learning orientation:** The cloud provider's core capabilities, know-how and absorptive capacity and its ability to leverage them. Learning capability includes both core skills and competences and the provider's ability to acquire new knowledge - also known as absorptive capacity. This absorptive capacity includes both technological expertise, such as the ability to generate new technologies, and market pioneering expertise, which can determine the commercial success of these technologies.
- **Location of data:** The location of data centres and the potential impact on data privacy and security. This factor is found in the cloud literature and can be a decisive factor in the battle for the cloud platform. If a provider is not compliant, there could be drastic legal consequences and a threat to data security and privacy.

4.2.2. Characteristics of the Cloud Platform

This category relates to the characteristics of the cloud platform. If a Cloud provider scores well on this, it means that their Cloud platform outperforms the platform of their competitors.

- **Technological superiority:** Platform design as having features that allow this design to outperform other traditional and competing designs (Schumpeter, 1980). This could attract customers by having a more advanced platform with features that competitors do not have.
- **Compatibility:** The compatibility of the organisation's existing systems and infrastructure with cloud services. This refers to the alignment of related entities to make them work together (Vries, 2013). When a platform is compatible, it is designed to be easily integrated into the existing infrastructure.
- **Complementary goods:** Substitute programs or products that together fulfil a common want. These are the other goods needed to successfully commercialise the platform. An example is products related to Office 365 in combination with Azure.
- **Flexibility:** Incremental costs and time required to adapt the platform due to new developments in technology. In general, this includes any changes to the cloud platform to meet customer needs.
- **Scalability:** The ability to easily scale up or down the amount of resources used as needed. Especially consider the speed and ease of scaling up. This may be a factor for financial institutions to consider in their vendor selection process.
- **Complexity:** The degree of complexity of the platform when using cloud services. This relates to the user-friendliness of the platform. If a platform has many advanced features, yet is difficult to work with, this can still be detrimental to its success.

- **Security Privacy:** The level of security and privacy of data stored in the cloud. From the regulator's point of view, Dutch financial institutions have to comply with a huge number of security and privacy requirements, see section 3.2. This is therefore an important factor when choosing a platform. If providers do not meet these, it is often already a no-go.
- **Availability:** The ability to have stable access to data and cloud services anywhere with an internet connection. For financial institutions, keeping IT systems working is also crucial. Incidental failures can quickly lead to serious problems, as sensitive information could be out in the open.

4.2.3. Cloud provider support strategy

This category relates to the strategies that the cloud provider can use to outperform their competitors.

- **Pricing strategy:** Actions of strategic pricing taken by company(s) to achieve market share to influence the dominance process. This has everything to do with the actions taken by the cloud provider to create market share by strategically pricing cloud-related products (Adams, 1996). This could include lowering prices to increase the platform's installed base to make their platform more attractive.
- **Timing of entry:** Moment at which a platform is introduced to the market. For example, early entry may mean that the provider can attract many customers early on who are less likely to switch later. On the other hand, it can also mean high investment costs and less market information in the early stages. Late entrants may also have a disadvantage because the market is already formed, so to speak, and customers are less likely to switch to other cloud providers.
- **Marketing Communications:** All actions to influence customer expectations. This can be important to inform customers about their own opportunities and/or future updates. This will keep customers informed and potentially attract new customers.
- **Distribution strategy:** Strategy used by the company(s) to distribute the format in the market. This refers to how the provider intends to distribute its platform across the market. This includes possible partnerships with other companies to implement or sell their platform. A good distribution strategy can accelerate platform adoption.
- **Commitment:** The amount of dedication and effort a company is willing to invest in promoting and supporting their platform. When a platform is in the early stages of its development and therefore generates little revenue, it is important that the provider remains committed to supporting and maintaining their platform. This can continue to be important in later stages to retain customers.

4.2.4. Other stakeholders

This category relates to stakeholders outside the group of cloud providers.

- **Current installed base:** The current number of specific cloud platforms implemented in companies in the industry. This can also be defined as the number of users of the technology, referring to a specific cloud platform. As we focus on the Dutch financial sector in this study, this factor refers to the number of cloud platforms of a specific provider currently in use within this sector. When the market is affected by network externalities, the current installed base will have an effect on platform adoption.
- **Big Fish:** Presence and actions of a large company with significant influence in the industry. This refers to a player (other than cloud providers) that can have a lot of influence by promoting or financially supporting a cloud platform. They may also have enormous buying power, so they can individually ensure that a platform becomes dominant (Suárez and Utterback, 1995).
- **Regulator:** Presence of regulatory bodies and actions taken by them that influence the battle. Within this battle, these may include regulators, such as DNB and AFM, or other government agencies that may enact certain laws to influence the outcome of the battle. Ultimately, the outcome will no longer be a pure market outcome (Axelrod et al., 1995).
- **Suppliers:** Suppliers of complementary goods. These are suppliers that produce complementary goods or services offered together with a cloud platform. Think of this battle strategic and implementation partners, who indirectly offer a particular platform and everything around it. Through these channels, cloud providers can build market share and thus pursue a system lock-in strategy (Malone et al., 2003).

- **Network of stakeholders:** The characteristics of the stakeholder network. This includes the size of the network, its diversity and strength. This relates to the network of cloud providers within the industry. When a particular cloud provider has a larger network with more power, their cloud platform is also more likely to become dominant within the industry.

4.2.5. Market characteristics

This category relates to market forces, over which the cloud providers have no influence. They simply exist and can influence the outcome of this battle.

- **Bandwagon effect:** If other users adopt a particular Cloud platform, others will tend to follow. This often has to do with the rationale for availability of information (Vries, 2013). In this regard, companies will wait for their competitors' choices and experiences before taking the same route.
- **Network externalities:** Network externalities refers to the increase in utility that occurs when more users use the same Cloud platform. A common example is the mobile phone where utility (the ability to connect with others) increases when more users adopt the phone. In this battle, for example, utility may increase when more companies within the industry use the same Cloud platform, due to smoother communication, for example.
- **Number of options available:** Number of options that can replace the cloud platform. This refers to the number of competing cloud platforms within the financial sector. The more competitors there are, the less likely a particular platform is to become dominant.
- **Uncertainty in the market:** Level of uncertainty in the market affecting the company's commitment to support the cloud platform. This effect affects both the provider and the customer. If the economy worsens, the cloud provider is likely to put less effort and money into maintaining and supporting their platform. Moreover, economic uncertainty may also reduce customer demand.
- **Rate of change:** The overall speed of change in technology, market and industry. This refers, for example, to the speed at which new generations of the cloud platform or new features are introduced into the platform. When this speed of change is high, it affects the desirability of committing to a format (Lee et al., 1995). As a result, users are less likely to commit to a particular platform and providers' commitment to support and guide a specific platform will decrease.
- **Switching costs:** The costs incurred when switching from the current Cloud platform to another platform. In this battle, you can think, for example, of the costs of converting IT systems and moving data, but also of the costs of retraining staff to a new format. When switching costs are high with a platform, it is also more likely that customers will be less likely to choose it and that this platform will become dominant.

5

Analyses and Results

In this chapter the results of the BWM are presented. As discussed in section 2.3, 13 Cloud experts at various Dutch financial institutions were interviewed. In these interviews, the experts were asked to compare the categories and associated factors according to the BWM methodology, explained in section 2.1.2. They were also asked to compare the three most popular cloud platforms (AWS, Azure and Google) with the same method on the same factors. In the following sections, the results of the two different parts are presented and discussed.

5.1. Factors

This section presents the results of the pairwise comparison of the different categories and factors. First, the consistency levels of the experts' responses are presented. Next, the pairwise comparison analyses of the different categories are discussed and then the strength of the relevant factors are further discussed. The results of each interview are compiled and these are discussed in the sections below. The complete results for each interview can be found in Appendix C.

5.1.1. Consistency ratio

Section 2.1.2 shows that problems may arise if the consistency levels of the answers of the experts are too high. The maximum acceptable value of this consistency level, also known as associated threshold, depends on the number of factors within a given category and the ranking scale used, see Table 2.1. Below you can see the results of the interviews.

Table 5.1: Results Consistency Ratio's Factors

		Category				
Int	**Group comparison**	**Characteristics of the Cloud provider**	**Characteristics of the Cloud Platform**	**Cloud provider support strategy**	**Other stakeholders**	**Market characteristics**
1	0,2000	0,2143	0,2143	0,1905	0,1905	0,2000
2	0,1667	0,2857	0,2857	0,2000	0,1071	0,1071
3	0,1667	0,1667	0,2143	0,2000	0,1333	0,1905
4	0,2000	0,1905	0,2143	0,1905	0,2000	0,1905
5	0,1905	0,2000	0,1500	0,2143	0,1190	0,2000
6	0,2083	0,2000	0,2083	0,2143	0,2143	0,2143
7	0,1786	0,2917	0,2143	0,2857	0,2619	0,3000
8	0,1667	0,1905	0,3095	0,1667	0,2639	0,1190
9	0,1667	0,1190	0,3000	0,2000	0,0476	0,2000
10	0,1528	0,1667	0,2222	0,2222	0,1667	0,2222
11	0,2143	0,1429	0,2083	0,2083	0,1333	0,1528
12	0,1333	0,2000	0,2000	0,1000	0,1190	0,2143
13	0,1667	0,2917	0,2000	0,1667	0,2000	0,2083

Green Expert interviews
Yellow Group comparison
Blue Categories

Based on table 2.1 with the corresponding threshold values and the individual results of the experts in table 5.1, one can conclude that all the answers of each expert in the group comparison and categories have an acceptable level of consistency. Thus, this will not pose any further problems for the reliability of the subsequent analyses.

5.1.2. Group comparison

In the interviews, the experts first compared the different categories. Based on these comparisons, weights were calculated for each category, indicating their relevance for cloud platform adoption within this sector (see appendix C for individual interview results). Table 5.2 shows the normalised geometric average weights of each category.

Table 5.2: Assigned weights of categories by experts

Category	**Average Weight**	**Ranking**
Characteristics of the Cloud Platform	0,3046	1
Characteristics of the Cloud provider	0,2278	2
Cloud provider support strategy	0,1759	3
Market characteristics	0,1740	4
Other stakeholders	0,1177	5

Green Firm level categories
Yellow Environmental category

Table 5.2 shows that *Characteristics of the cloud platform* (0,3046) and *Characteristics of the cloud provider* (0,2278) are, according to the experts, the most important categories for this cloud platform battle. This is followed by *Cloud provider Support strategy* (0,1759) and *Market Characteristics* (0,1740), and the least important category is *Other stakeholders* (0,1177).

The validation interviews, show that all IT/cloud experts agree with this ranking. This is due to the fact that financial institutions often look at the specific platform and the provider first. If the provider does not meet the strict requirements, then it is already a no-go. If that assurance is there, only then do they look at other issues related to the other three categories. *Other stakeholders* come last, as financial institutions are not easily influenced by other parties. The only factor in this category that is very important is *Regulator*, because they supervise all financial institutions in the Netherlands. But I will discuss this factor later in this chapter.

5.1.3. Strength of relevant factors

Besides comparing the different groups, the experts were also asked to compare the corresponding factors within each group, see appendix C for the complete weights per interview. Based on these results, local average weights per factor in a category are calculated. These are the local normalised geometric averages of all interviews per factor. By then multiplying these local average weights by the weight of the corresponding category (table 5.2), the global average weights are calculated. These global average weights ultimately determine the final ranking of all factors. See table 5.3 for an overview of all average weights and the ranking.

Table 5.3: Final BWM results factor comparison

#	Factors	Local Average Weight	Global Average Weight	Global ranking
Firm level factors				
Characteristics of the Cloud provider		**0,2278**		
1	Financial strength	0,1274	0,0290	**14**
2	Brand reputation and credibility	0,2821	0,0642	**2**
3	Operational supremacy	0,2032	0,0463	**8**
4	Location of data	0,2054	0,0468	**7**
5	Learning orientation	0,1819	0,0414	**10**
Characteristics of the Cloud Platform		**0,3046**		
6	Technological superiority	0,0819	0,0249	**19**
7	Compatibility	0,1709	0,0520	**5**
8	Complementary goods	0,0753	0,0229	**22**
9	Flexibility	0,0835	0,0254	**18**
10	Scalability	0,0966	0,0294	**13**
11	Complexity	0,0704	0,0215	**24**
12	Security & Privacy	0,2643	0,0805	**1**
13	Availability	0,1571	0,0479	**6**
Cloud provider support strategy		**0,1759**		
14	Pricing strategy	0,3109	0,0547	**3**
15	Timing of entry	0,1293	0,0228	**23**
16	Marketing Communications	0,0920	0,0162	**28**
17	Distribution strategy	0,1580	0,0278	**17**
18	Commitment	0,3098	0,0545	**4**
Other stakeholders		**0,1177**		
19	Current installed base	0,2020	0,0238	**21**
20	Big Fish	0,1204	0,0142	**29**
21	Regulator	0,3730	0,0439	**9**
22	Suppliers	0,1652	0,0194	**25**
23	Network of stakeholders	0,1395	0,0164	**27**
Environmental factors				
Market characteristics		**0,1740**		
24	Bandwagon effect	0,1102	0,0192	**26**
25	Network externalities	0,1651	0,0287	**15**
26	Number of options available	0,1432	0,0249	**20**
27	Uncertainty in the market	0,1601	0,0279	**16**
28	Rate of change	0,2048	0,0356	**12**
29	Switching costs	0,2165	0,0377	**11**

Green Firm level factors
Yellow Environmental factors

Based on the global average weights in table 5.3, one can conclude that the five most important factors in order are: 1) *Security & privacy* (0,0805), 2) *Brand reputation and credibility* (0,0642), 3)

Pricing strategy (0,0547), 4) *Commitment* (0,0545) and 5) *Compatibility* (0,0520). The five least important factors are in order: 29) *Big Fish* (0,0142), 28) *Marketing communication* (0,0162), 27) *Network of stakeholders* (0,0164), 26) *Bandwagon effect* (0,0192) and 25) *Suppliers* (0,0194). These five most and least important are further discussed in the following sections. Based on the third round of validation (appendix A.3), other influencing factors may also be discussed.

Top influencing factors

Table 5.3 shows that *Security & privacy*, *Brand reputation and credibility*, *Pricing strategy*, *Commitment* and *Compatibility* are the five most important factors for cloud platform adoption in the Dutch financial sector. Below, each factor is briefly discussed.

- **Security & Privacy:** From the regulator's point of view, this factor should always be a top priority. cloud providers have to comply with certain regulations and if they do not, it is automatically a no-go. The ever-increasing cyber security threats, such as ransomware, also mean that financial institutions need to do a lot of risk mitigation when outsourcing (see appendix A.3).
- **Brand reputation and credibility:** As shown in the past (Axelrod et al., 1995), the results of the expert interviews also show that this factor is very important for cloud platform adoption among financial institutions. They are under constant scrutiny from regulators, making it important that they can trust their cloud provider. In addition, it can be disastrous for these institutions if their cloud platform has problems. Their reputation goes down and sensitive information may be out on the street.
- **Pricing strategy:** This factor is very important because it can help gain strength within the organisation. If a provider follows attractive pricing strategies, financial institutions can achieve their goals faster. That way, they can negotiate for the long term and thus become more advantageous in the long run. However, this is less of an issue for smaller financial institutions, as they purchase a smaller cloud package and can therefore negotiate less effectively (see appendix A.3).
- **Commitment:** Cloud strategy costs a lot of money, so you also need reliability in the partnership. Financial institutions sign contracts for the long term, so if there are problems they want quick support. Also with new cloud developments. So it is very important that the provider is and stays involved.
- **Compatibility:** This factor is also very important, as the integration process runs more smoothly if the implementation of the platform takes little time and money. Often, financial institutions already have an existing infrastructure, so it is nice if the cloud platform integrates well with it.

Compared to the literature review presented in the previous chapter (see Table 4.1), it is clear that the factors *Security & Privacy*, *Pricing strategy* and *Compatibility* appear frequently in the literature on cloud adoption worldwide. This suggests that these factors are of great importance for cloud adoption worldwide and are not just limited to the specific sector analysed in this study.

Interestingly, *Brand reputation and credibility* and *Commitment* received less attention in the reviewed articles, suggesting that for Dutch financial institutions, it is crucial that the cloud provider has a reputable image and shows a strong commitment throughout the cloud transformation process. Overall, based on the literature, these factors do not seem extremely important for cloud adoption in general.

Furthermore, it is remarkable that *Technological superiority* and *Regulator* are frequently discussed in the literature on cloud adoption, but do not emerge as critical factors in this study. This may be because Dutch financial institutions place more emphasis on the security aspect of the cloud platform than on its technological superiority. This distinction may differ from cloud adoption practices in general. Although *Regulator* is still considered important, they receive less attention in this study because their category relevance is lower, see Table 5.2.

Least influencing factors

Table 5.3 shows that *Big Fish*, *Marketing communication*, *Network of stakeholders*, *Bandwagon effect* and *Suppliers* are the five least important factors for cloud platform adoption in the Dutch financial sector. Below, each factor is briefly discussed.

- **Big Fish:** This factor is not important because financial institutions do not really look at big fish outside their competitors and regulators. This is because these big fish and the financial sector

are so different organisationally and in terms of regulations that they prefer not to look at them. Companies outside the financial sector are much freer in their actions and are less concerned with security and privacy. This contradicts the literature, which indicates that companies can indeed be influenced by Big Fish, whose enormous buying power can individually ensure that a platform becomes dominant (Suárez and Utterback, 1995).

- **Marketing Communications:** Experts agree that this is not an important factor. Decisions when selecting a cloud vendor are not made based on marketing, quite the contrary. This kind of marketing is seen as annoying spam. Rather, choices are made based on requirements from regulators. However, they do admit that the cloud vendor may have indirect influence because they are on their mind.
- **Network of stakeholders:** This factor is related to the explanation of *Bandwagon effect*. Financial institutions initially look at themselves and their own needs before looking at the specific provider's network.
- **Bandwagon effect:** This factor is less important because financial institutions are generally more self-focused. They initially look for a cloud provider that suits them and then ask how many other institutions they already work with. So this factor is a consequence rather than being seen as decisive in the first place.
- **Suppliers:** As discussed in previous factors, financial institutions initially choose a cloud provider and only then everything that follows. Suppliers, for example, are not important initially, but can play an important role in a successful partnership after the choice of provider.

Table 4.1 of the literature review in the previous chapter shows that the factors *Big Fish*, *Marketing Communications* and *Suppliers* are minimally present in the global literature on cloud adoption. This implies that these factors have little significance for cloud adoption on a global scale, and not only in the specific sector analysed in this study. Moreover, the factors *Network of stakeholders* and *Bandwagon effect* are slightly more present in the literature, but still relatively unimportant. Therefore, it can be concluded that the five least important factors identified in this study correspond to the general perspective on cloud adoption.

Interestingly, *Location of data* is rarely mentioned in the literature, but emerges as a crucial factor in this study. This can be attributed to the stricter regulations on data centre location in the EU compared to other parts of the world. Moreover, *Distribution strategy* and *Uncertainty in the market* are hardly discussed in the literature, but are of moderate significance in this study. This may be because financial institutions prioritise strong relationships with distribution partners and require cloud platforms to be resilient to market uncertainties. They need to be confident that the platform will continue to function during disruptions.

Other influencing factors

Based on the validation interviews in Round 3 (see appendix A.3), a number of other influencing factors also emerged that are worth mentioning. Below, each factor is briefly discussed.

Important factors:

- **Location of data:** This factor is related to *Security & Privacy* and is very important when choosing a cloud platform. If a cloud provider's data centres are not located within the EU or preferably in the Netherlands, then their customers' data is at risk and this provider is not really attractive.
- **Operational supremacy:** This is one of the most important factors, as financial institutions often enter into long-term contracts of several years with cloud providers (see appendix A.3). They would like the providers to stay involved during those years and be able to provide support if there are problems. It is also important that the systems remain maintained and thus up-to-date.
- **Regulator:** This factor is also very important because the regulator has a lot of influence on security and privacy requirements within the industry. If providers do not meet these, the regulator intervenes. Currently, however, most cloud providers meet these requirements, which is why it did not make it into the top five.

Not important factors:

- **Complexity:** This factor is highly dependent on different interpretations. The complexity of a cloud platform is not necessarily important, but indirectly it is, depending on how knowledgeable

the financial institutions are (see appendix A.3). For example, if an institution has many experts on Azure, AWS will be seen as very complex, but vice versa, Azure will again be seen as complex. So complexity is not directly very important, but indirectly through the knowledge the institutions have in-house.

- **Flexibility:** What is striking is that financial institutions generally do not care that much about new developments in the field of cloud. What emerges from the interviews is that security comes first and that is why they do not experiment much with new features. Only when these features are proven to be secure, they may consider it.
- **Current installed base:** For financial institutions, this factor is generally not very important. As discussed earlier, they mainly look at themselves before choosing a cloud platform. When making this choice, however, it can be a factor to consider. For example, if a particular platform is hardly used in the industry, it is also less attractive for financial institutions to choose this provider.
- **Timing of entry:** Experts had estimated this factor to be slightly less important. If a cloud provider has entered the market before, it does not immediately mean that a financial institution finds this provider more attractive. What matters is what they offer now, not how long they have been around. The stability of the platform is paramount.

5.2. Platform comparison

This section discusses the platform comparison. As discussed in chapter 1, it was decided to compare the three most popular cloud platforms (AWS, Azure and Google) based on the relevant factors. All experts were asked in the interviews to score the platforms on each factor, see complete results in appendix D. This was again done using the BWM, discussed in section 2.1.2.

5.2.1. Consistency ratio

Section 2.1.2 shows that problems can arise if the consistency level of the experts' answers is too high. The maximum acceptable value of this consistency level, also known as associated threshold, depends on the number of alternatives within a given category and the ranking scale used, see Table 2.1. This study examines the three most popular platforms (AWS, Azure and Google). This means that three alternatives have been used and the associated threshold value thus only depends on the scale used by the experts. The consistency ratio's per interview can be seen in appendix D.

Based on the table 2.1 of simplified thresholds and the individual expert results in the annex D.1, it can be concluded that all answers of the experts have acceptable consistency levels. This therefore poses no further problems for the reliability of subsequent analyses.

5.2.2. Final outcome battle

As discussed in section 2.1.2, the experts were also asked to compare the three most popular cloud platforms (AWS, Azure and Google) on each factor. The same BWM method was used for this comparison, where the cloud platforms served as criteria and were compared on each factor. Based on this, the platforms were given a performance score on each factor per interview, see appendix D. The normalised geometric averages of all these interview are presented in Table 5.4.

By multiplying the performance scores by the average global weights from table 5.3, the weighted scores per platform per factor are calculated. The final result of the battle for the cloud platform can finally be determined by adding up those weighted scores per platform. See the table below for the results.

Table 5.4: Final outcome cloud platform battle

Factors		Cloud Platform					
		AWS		Azure		Google	
Firm level factors		**Performance score**	**Weighted score**	**Performance score**	**Weighted score**	**Performance score**	**Weighted score**
Characteristics of the Cloud provider							
1	Financial strength	0,3708	0,0108	0,4642	0,0135	0,1650	0,0048
2	Brand reputation and credibility	0,3782	0,0243	0,4773	0,0307	0,1445	0,0093
3	Operational supremacy	0,3118	0,0144	0,4772	0,0221	0,2110	0,0098
4	Location of data	0,3059	0,0143	0,4626	0,0216	0,2315	0,0108
5	Learning orientation	0,3641	0,0151	0,4000	0,0166	0,2359	0,0098
Characteristics of the Cloud Platform							
6	Technological superiority	0,3528	0,0088	0,4184	0,0104	0,2288	0,0057
7	Compatibility	0,2693	0,0140	0,5571	0,0290	0,1736	0,0090
8	Complementary goods	0,2329	0,0053	0,5669	0,0130	0,2002	0,0046
9	Flexibility	0,3120	0,0079	0,3505	0,0089	0,3375	0,0086
10	Scalability	0,3470	0,0102	0,3272	0,0096	0,3259	0,0096
11	Complexity	0,3658	0,0078	0,3562	0,0076	0,2780	0,0060
12	Security & Privacy	0,3132	0,0252	0,5376	0,0433	0,1492	0,0120
13	Availability	0,2901	0,0139	0,3485	0,0167	0,3614	0,0173
Cloud provider support strategy							
14	Pricing strategy	0,3866	0,0211	0,3028	0,0166	0,3106	0,0170
15	Timing of entry	0,5885	0,0134	0,3038	0,0069	0,1077	0,0025
16	Marketing Communications	0,2911	0,0047	0,5086	0,0082	0,2002	0,0032
17	Distribution strategy	0,2610	0,0073	0,5632	0,0157	0,1759	0,0049
18	Commitment	0,3379	0,0184	0,4282	0,0233	0,2340	0,0127
Other stakeholders							
19	Current installed base	0,3779	0,0090	0,4960	0,0118	0,1261	0,0030
20	Big Fish	0,3241	0,0046	0,4791	0,0068	0,1968	0,0028
21	Regulator	0,2965	0,0130	0,5888	0,0258	0,1147	0,0050
22	Suppliers	0,2752	0,0053	0,5321	0,0103	0,1927	0,0037
23	Network of stakeholders	0,2572	0,0042	0,6086	0,0100	0,1342	0,0022
Evironmental factors							
Market characteristics							
24	Bandwagon effect	0,3384	0,0065	0,4492	0,0086	0,2124	0,0041
25	Network externalities	0,3632	0,0104	0,4563	0,0131	0,1805	0,0052
26	Number of options available	0,2963	0,0074	0,4485	0,0112	0,2552	0,0064
27	Uncertainty in the market	0,3986	0,0111	0,4440	0,0124	0,1574	0,0044
28	Rate of change	0,3036	0,0108	0,3676	0,0131	0,3288	0,0117
29	Switching costs	0,3916	0,0148	0,2211	0,0083	0,3873	0,0146
Total			**0,3342**		**0,4452**		**0,2206**
Ranking			**2**		**1**		**3**

Green Firm level factors
Yellow Environmental factors

The table above shows that Azure (0.4452) achieved the best score on all factors. In second place is AWS (0,3342) and in last place is Google (0,2206).

The three experts in the validation interviews (see appendix A.3) unanimously agreed that this ranking and interrelationship is something they had expected. They indicated that Azure has currently taken more steps to meet regulators' wishes and requirements. The Dutch financial sector often opts for security rather than experimentation. However, they did indicate that Azure is mainstream in Europe, but that financial institutions overseas more tend to move to AWS or Google Cloud. As a result, it is often important for large Dutch international financial institutions to have some operations with another cloud provider, also called a multi cloud strategy. This is to reduce the chances of being totally dependent on a cloud provider and make it easier to switch providers.

6

Conclusion and recommendations

This chapter first answers the research questions. Next, the theoretical and practical contributions of this research are discussed. Third, the limitations of this study and recommendations for further research are presented. Finally, the reflection considers the findings and their connection to the EPA MSc program.

6.1. Answers to research questions

Chapter 1 identified a lack of understanding of the implementation of complex innovations, such as cloud platform business models, at financial institutions. These institutions have often struggle with how to design and manage this type of technology (Das, 2019). This study aimed to to understand the key factors influencing the suitability of a cloud platform within the cloud platform battle in the Dutch financial sector. By taking into account the unique characteristics and regulations of this sector and identifying the key influencing factors, this study aimed to identify a suitable cloud platform.

Based on this objective, the following main research question was formulated:

What are the key influencing factors that determine the adoption of a cloud platform within the cloud platform battle within the Dutch financial sector?

To answer this main research question, several sub-questions were formulated. The first sub-question read: *What is the current state of Cloud in the Dutch financial sector?* In order to answer this sub-question, literature research was conducted and exploratory interviews were held with several IT/Cloud experts within the Dutch financial sector, see chapter 2. Chapter 3.1 shows that the global cloud platform market in the financial sector will grow significantly in the coming years with an annual growth rate of 12.4% and an expected increase from $23.7 billion in 2022 to $90.1 billion in 2032. In this, AWS (Amazon) is the global market leader, closely followed by Azure (Microsoft), with Google a distant third. In the Dutch financial sector, Azure and AWS are almost equal in market share (+/- 40%), with Google lagging far behind (+/- 15%). Furthermore, Azure is more often adopted by large financial institutions and AWS and Google more often by somewhat smaller financial institutions.

To answer the second sub-question, *What policy regulations currently affect the adoption of cloud platforms technologies in the Dutch financial sector?*, a literature review was again conducted and the participants in interview round 1 were also asked questions about this. Section 3.2 shows that there are several regulations that influence the adoption of Cloud platforms in the Dutch financial sector. For example, there are general regulations that have been around for some time, such as the General Data protection Regular (GDPR) and Network and the Information Systems Directive (NISD). But there are also more Cloud specific regulations, such as the ISO standards and the Digital Operational Resilience Act (DORA). Finally, based on all these regulations, The European Securities and Markets Authority (ESMA) published nine guidelines for financial institutions outsourcing their operations to Cloud Service Providers (CSPs) to ensure compliance and security. Consider drafting exit strategies and information security requirements, see all the guidelines in 3.2.

To answer the third sub-question, *What are relevant factors for the adoption of cloud platforms in the Dutch financial sector?*, another literature review was conducted and the participants in interview

round 1 were also asked questions about this. Van der Kaa's framework of 29 factors that can influence the outcome of a technology battle (van de Kaa et al., 2011) was the basis for this sub-question. Then, based on the three interviews and 26 reviewed articles, a final set of factors for the adoption of cloud platforms in the Dutch financial sector was created. Based on how often a particular factor was mentioned in the interviews and appeared in the literature, it was determined whether each factor was relevant enough to be included in the final set of factors. 24 factors from van der Kaa's framework proved relevant enough and five more factors related to cloud were added. In the end, a set of 29 relevant factors emerged, see table 4.2.

To answer the fourth sub-question, *What are the most important factors for the adoption of a cloud platform, using the Best-Worst Method?*, 13 interviews were conducted with different IT/cloud experts at different Dutch financial institutions. The interviewees were asked to compare the factors found in the previous sub-question by category based on relevance for the adoption of a cloud platform within their sector. This was done using the Best-Worst Method (BWM) (see section 2.1.2), after which the final set of relevant factors could finally be sorted by relevance (see table 6.1).

Table 6.1: BWM-factors: Average global weight and global ranking

Factors	Category	Average Global Weight	Global ranking
Security & Privacy	Characteristics of the Cloud Platform	0,0805	1
Brand reputation and credibility	Characteristics of the Cloud provider	0,0642	2
Pricing strategy	Cloud provider support strategy	0,0547	3
Commitment	Cloud provider support strategy	0,0545	4
Compatibility	Characteristics of the Cloud Platform	0,0520	5
Availability	Characteristics of the Cloud Platform	0,0479	6
Location of data	Characteristics of the Cloud provider	0,0468	7
Operational supremacy	Characteristics of the Cloud provider	0,0463	8
Regulator	Other stakeholders	0,0439	9
Learning orientation	Characteristics of the Cloud provider	0,0414	10
Switching costs	Market characteristics	0,0377	11
Rate of change	Market characteristics	0,0356	12
Scalability	Characteristics of the Cloud Platform	0,0294	13
Financial strength	Characteristics of the Cloud provider	0,0290	14
Network externalities	Market characteristics	0,0287	15
Uncertainty in the market	Market characteristics	0,0279	16
Distribution strategy	Cloud provider support strategy	0,0278	17
Flexibility	Characteristics of the Cloud Platform	0,0254	18
Technological superiority	Characteristics of the Cloud Platform	0,0249	19
Number of options available	Market characteristics	0,0249	20
Current installed base	Other stakeholders	0,0238	21
Complementary goods	Characteristics of the Cloud Platform	0,0229	22
Timing of entry	Cloud provider support strategy	0,0228	23
Complexity	Characteristics of the Cloud Platform	0,0215	24
Suppliers	Other stakeholders	0,0194	25
Bandwagon effect	Market characteristics	0,0192	26
Network of stakeholders	Other stakeholders	0,0164	27
Marketing Communications	Cloud provider support strategy	0,0162	28
Big Fish	Other stakeholders	0,0142	29

Green Firm level factors
Yellow Environmental factors

Table 6.1 shows that the factors: 1) *Security & privacy*, 2) *Brand reputation and credibility*, 3) *Pricing strategy*, 4) *Commitment* and 5) *Compatibility*, are the most important factors for cloud platform adoption. An explanation was sought by presenting the results and asking their thoughts to a num-

ber of IT/Cloud experts in the third and final validation interview round, see section 2.5. The experts all indicated that from a regulator's perspective, *Security & Privacy* are top priorities and regulatory compliance is essential. *Brand reputation and credibility* are also important, as financial institutions are under constant scrutiny from regulators and need to trust their cloud provider. *Pricing strategy* is important to gain power within the organisation and negotiate for the long term. *Commitment* is crucial for partnership reliability, and *Compatibility* with existing infrastructure makes the integration process smoother. In addition, the literature review in chapter 4 shows that *Security & Privacy*, *Pricing strategy* and *Compatibility* are also important factors for cloud adoption globally. Interestingly, *Brand reputation and credibility* and *Commitment* receive less attention in the literature, however, they are crucial for Dutch financial institutions. This suggests that for Dutch financial institutions, it is more crucial that a cloud provider has a reputable image and shows a strong commitment throughout the cloud transformation process, compared to other sectors.

To answer the last sub-question, *Which cloud platform is the most suitable for the Dutch financial sector?*, the 13 interviewees in Round 2 were also asked to score the three most popular cloud platforms (AWS, Azure and Google) on each factor. Again, this was done using the Best-Worst Method and the results can be seen in table D.3. By multiplying these scores by the factor weights found in the previous sub-question, one arrives at the weighted scores per cloud platform on a given factor. Adding up these weighted scores per platform, one finally arrives at the total weighted score per platform, see table 5.4. Here you can see that *Azure* (0.4452) has the highest score, making it the most suitable for the Dutch financial sector. Followed by *AWS* (0.3342) in second place and *Google* (0.2206) with the lowest score in last place. From this it can be concluded that *Azure* is the most suitable cloud platform for the financial sector. The three experts in the validation interviews agreed that the ranking of Azure and its relationship with regulators is not surprising, as Azure has taken more steps to meet regulatory requirements. They noted that in the Dutch financial sector, security is preferred over experimentation. While Azure is popular in Europe, overseas financial institutions prefer AWS or Google Cloud. Therefore, large Dutch international financial institutions often opt for a multi-cloud strategy to reduce their dependence on a single provider and make it easier to switch providers when needed.

In the end, it can be concluded, and thus answer the main research question, that the factors: 1) *Security & privacy*, 2) *Brand reputation and credibility*, 3) *Pricing strategy*, 4) *Commitment* and 5) *Compatibility*, are the key influencing factors that determine the adoption of a cloud platform within the cloud platform battle within the Dutch financial sector. Based on these factors and the platform comparison, it can then be determined that the cloud platform *Azure* is currently the most suitable for the Dutch financial sector and thus also has the greatest chance of becoming dominant within the sector.

6.2. Contributions

This section discusses first the theoretical and then the practical contributions.

6.2.1. Theoretical contributions

This research contributed to previous literature on cloud platform adoption in several ways. First, the research builds on van der Kaa's earlier framework of factors that can influence the outcome of a technology battle (van de Kaa et al., 2011). This framework is highly standardized and can be applied to multiple technology battles, but has never been adapted to a specific cloud platform battle. In the end, based on 26 reviewed articles and exploratory interviews with IT/Cloud experts, only 24 of the 29 factors from van der Kaa's framework (van de Kaa et al., 2011) were found to be relevant to this particular cloud platform battle. In addition, five new factors related to cloud platform adoption were added to the framework. This ultimately resulted in a new set of 29 factors that can influence the outcome of a cloud platform battle (see table 4.2).

Second, the BWM approach was used for the first time to identify the success factors for cloud platform adoption in the Dutch financial sector. There has been previous research on the factors for cloud adoption in the financial sector, but the factors of cloud platform adoption in the Dutch financial sector are never been investigated. The major differences here are that the factors in this research focus on cloud provider characteristics rather than users and that the research focuses only on cloud platform adoption in the Dutch financial sector. The geographical location can have a lot of influence on the choice of financial institutions, as they depend on (inter)national regulations on cloud platform

adoption (see section 3.2).

Third, the BWM approach is used for the first time to compare cloud platforms based on the listed factors. There has been previous research on the differences between certain cloud platforms, but this has never been investigated using the BWM. With this method, the three most popular cloud platforms (AWS, Azure and Google) could be quantitatively compared on every relevant factor found in section 5.

Finally, the identification of relevant factors for cloud platform adoption and a comparison of cloud platforms has not previously been combined to find a most suitable platform for a particular industry. As mentioned earlier, there has been previous research on relevant factors for cloud adoption or the differences between certain cloud platforms, but this has not been combined before. Combining these can help to specifically compare cloud platforms for a particular sector.

6.2.2. Practical contributions

Besides the theoretical contributions, there are also a number of practical contributions, to which this research has contributed. First, this research may lead to some policy implications. For instance, it is interesting for policymakers to see which factors are most important for financial institutions to adopt a cloud platform. Obviously, Dutch government agencies, such as the DNB and AFM, strive to ensure that financial institutions choose the most secure option. By adjusting regulations for certain cloud providers so that they meet the most important factors, they can push financial institutions towards the desired cloud provider. In addition, based on the cloud platform comparison, they can check whether the most suitable platform resulting from this study complies with all regulations. If they does not meet this, the government can still impose regulations on these providers before it is too late.

Second, mapping out regulations and guidelines related to cloud platform adoption can help financial institutions in the Netherlands get an overview of the related policy arena. This overview can make financial institutions less likely to forget or overlook regulations.

Third, identifying the most relevant factors for the adoption of a cloud platform within the industry can enable Dutch financial institutions to better assess cloud providers. Because they now know which factors are most important, they can score cloud providers in the future on the most important factors first. Now, they still find it difficult to identify key criteria for choosing a cloud provider.

Third, the comparative study of the three popular cloud platforms (AWS, Azure and Google) can help Dutch financial institutions make a choice for one of these three platforms. Currently, this is difficult because of the complexity of the platforms.

Fourth, using the BWM approach, the proposed framework can also be used to compare other cloud platforms. This is possible because the framework with factors is not related to specific cloud platforms and can be applied to all kinds of different cloud platforms. This is interesting for financial institutions so it can help them decide which platform to adopt. But this can also be interesting for government agencies, as they can then test new cloud providers on the market and thus make an expectation on whether this cloud provider will become successful within the Dutch financial market.

Last, the factors identified in the framework can be used to determine successful strategies for cloud providers looking to enter the Dutch financial market. As a result of this research, cloud providers have a better understanding of what Dutch financial institutions consider important factors when choosing a cloud platform.

6.3. Limitations and recommendations

This section discusses limitations and recommendations for further research. First, there is a possibility that experts may have misinterpreted the definitions of the categories and factors. This was obviously tried to avoid by sending the list of definitions in advance and briefly explaining the factors during the interviews. But there is always a chance that the experts had barely read through the factors and their definitions and misinterpreted them during the interview. In the end, I tried to minimise the chances of this happening. In future research, the experts can be double-checked by asking them some control questions.

Second, I discovered during the interviews that some factors were related to each other, such as *Security & Privacy* and *Regulator* or *Learning orientation* and *Flexibility*. This was because they had similarities but belonged to a different category. *Security & Privacy*, for example, belongs to *Characteristics of the cloud platform* and *Regulator* to *Other stakeholders*. Future research might investigate

whether certain factors correlate with each other before including them in the BWM.

Third, many Cloud experts said they had a lot of knowledge about Azure, slightly less knowledge about AWS and even less about Google. This ultimately prevented many experts from comparing these platforms on certain factors. Also, their better knowledge of Azure probably made them a bit more biased towards this provider. These missing scores and possibly biased experts ultimately make this comparison of cloud platforms a bit less reliable. In future research, more interviews could be conducted with experts who have comparable knowledge about all three cloud platforms, making this comparison more reliable.

Fourth, this study conducted interviews with 13 experts, some of whom were from the same company. Ideally, these should be more interviews with different backgrounds. This increases reliability and reduces the likelihood of biased results.

The fifth limitation is that there is no overall optimal solution with the BWM approach. Only the criteria and weight influence the final result, which in reality, of course, also depends on other factors, such as psychological factors. Future research, in addition to this study, could also investigate, for instance, psychological factors that may influence the choice of a cloud platform.

The final limitation of the study is that it focuses exclusively on the Dutch financial sector and the three most widely used cloud platforms (AWS, Azure and Google). The Dutch financial sector relies heavily on strict national and international (EU) IT regulations. In addition, cloud platforms may be popular here that are less popular in other parts of the world. To further explore this topic in future research, it would be interesting to conduct a similar study in a different geographical location or sector with different cloud platforms. This research is standardised so that this is possible. Instead of interviews with cloud experts from the Dutch financial sector, interviews could be conducted with cloud experts from other countries and sectors. This approach would allow the researcher to compare findings across different countries and/or sectors. Moreover, instead of comparing the three most popular cloud platforms, one could select three alternative platforms to compare.

6.4. Reflection

In this section, we discuss reflection on the findings and the link to the EPA MSc program.

6.4.1. Challenges

The most challenging part of my thesis was finding a topic. Before starting my thesis internship, I had deliberately not made a choice, as I could still come up with a mutually interesting topic with my colleagues and supervisor. However, after many exploratory discussions with my colleagues and supervisor, I found out that I had to make the choice myself. It was impossible to satisfy everyone's interests. I found out that cloud technology was of interest to everyone and decided to go ahead with it.

Then I came to the next pain point and that was choosing a method. I soon got a tip from a fellow student to first look at previous courses I found interesting and then apply the method discussed here to my topic. Then I soon came to the course *Technology Battles*, which I found very interesting at the time, and was able to frame my topic in such a way that I was going to research the battle between cloud platforms. This was quickly approved, allowing me to start.

Before starting my research, I was quickly told to start scheduling interviews right away. This ultimately made finding interviewees not a big problem. However, I found it difficult to prepare the interviews properly when I had not yet got that far with my writing. Fortunately, I knew the goals of the interviews, so I could make a good assessment. However, after a few interviews, I had to make a small adjustment to make the future interviews run more smoothly. In the end, I was able to successfully conduct the interviews and collect the data I needed. I also learnt to discuss the research steps with my company and university supervisor. This prevented problems in later stages.

6.4.2. Link to EPA MSc program

From an academic researcher's perspective, the present issue is relevant to the EPA curriculum and my specialisation, "*Emerging Technology-based Innovation & Entrepreneurship*, as it connects to several major challenges. The issue mainly relates to cybersecurity, privacy and innovation. The lack of proper guidance and monitoring of innovations makes financial institutions more vulnerable to threats, such as cyber-attacks, which can lead to the shutdown of critical systems and exposure of personal

data (Das, 2019). This research aims to explore ways in which established Dutch financial institutions can innovate responsibly, taking into account cyber security threats and ethical concerns. With the help of this research, Dutch financial institutions can better assess cloud providers and their cloud platform. They can use this framework to test cloud providers, so to speak. This contributes to responsible innovation within the sector and will minimise the likelihood of cyber threats, and thus endangering citizens' sensitive information. Furthermore, this research can contribute to the understanding of innovation in traditional financial firms with inflexible systems.

References

Adams, M. (1996). Norms, standards, rights. *European Journal of Political Economy*, *12*(2), 363–375. https://doi.org/10.1016/0176-2680(95)00022-4

Agarwal, R., Echambadi, R., Franco, A., & Sarkar, M. (2017). Knowledge Transfer Through Inheritance: Spin-Out Generation, Development, and Survival. Retrieved March 8, 2023, from https://journals.aom.org/doi/abs/10.5465/20159599

Alsmadi, D., & Prybutok, V. (2018). Sharing and storage behavior via cloud computing: Security and privacy in research and practice. *Computers in Human Behavior*, *85*, 218–226. https://doi.org/10.1016/j.chb.2018.04.003

Anderson, N. (2021). A Practical Introduction to Cloud Computing. Retrieved January 25, 2023, from https://eylearning.udemy.com/course/introduction-cloud-computing/

Asadi, S., Nilashi, M., Husin, A. R. C., & Yadegaridehkordi, E. (2017). Customers perspectives on adoption of cloud computing in banking sector. *Information Technology and Management*, *18*(4), 305–330. https://doi.org/10.1007/s10799-016-0270-8

Asatiani, A. (2015). Why Cloud? - A Review of Cloud Adoption Determinants in Organizations, 18.

Axelrod, R., Mitchell, W., Thomas, R. E., Bennett, D. S., & Bruderer, E. (1995). Coalition Formation in Standard-Setting Alliances [Publisher: INFORMS]. *Management Science*, *41*(9), 1493–1508. https://doi.org/10.1287/mnsc.41.9.1493

Baykara, S. (2020). PCI DSS Requirements. Retrieved January 23, 2023, from https://www.pcidssguide.com/pci-dss-requirements/

Brits, H., Cuijpers, G., Jonker, N., Lohuis, M., Roerink, R., & Zwemstra, A. (2021). Veranderend landschap, veranderend toezicht. *DNB*, 50.

Das, P. (2019). *Controlling disruptive and radical innovations in large-scale services firms* (Doctoral dissertation). Delft University of Technology. https://doi.org/10.4233/UUID:E889F189-DBD1-4D5C-8184-8456418D1886

DNB. (n.d.). Toezicht op financiële instellingen. Retrieved March 6, 2023, from https://www.dnb.nl/betrouwbare-financiele-sector/toezicht-op-financiele-instellingen/

ESMA. (2021). ESMA wijst met nieuwe richtsnoeren op beheersing risico's bij uitbesteding naar de cloud. Retrieved January 20, 2023, from https://www.afm.nl/nl-nl/sector/actueel/2021/juli/esma-richtsnoeren-uitbesteding-clouddiensten

European Commission. (2020). DORA (Digital Operational Resilience Act) proposal. Retrieved January 23, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0595&from=EN

FMI. (2021). Finance Cloud Market. Retrieved November 29, 2022, from https://www.futuremarketinsights.com/reports/finance-cloud-market

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, *35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

Gutierrez, J. A. (2019). The rise of FinTech in banking. Retrieved May 12, 2022, from https://www.russellbedford.com/latest/insight/the-rise-of-fintech-in-banking/

Hsu, C.-L., & Lin, J. C.-C. (2016). Factors affecting the adoption of cloud services in enterprises. *Information Systems and e-Business Management*, *14*(4), 791–822. https://doi.org/10.1007/s10257-015-0300-9

Hurwitz, K. (2019). 5 Barriers To Innovation In Digital Banking & How To Beat Them [Section: Project Management]. Retrieved April 28, 2022, from https://praxent.com/blog/innovation-in-banking-ideas-for-overcoming-challenges

ISO. (n.d.). ISO - ISO/IEC 27001 and related standards — Information security management. Retrieved January 23, 2023, from https://www.iso.org/isoiec-27001-information-security.html

Janakiram. (n.d.). Google Cloud Platform (GCP) Fundamentals for Beginners. Retrieved January 25, 2023, from https://eylearning.udemy.com/course/google-cloud-platform-gcp-fundamentals-for-beginners/

Jones, H. (2022). Banks in EU face tougher rules on using cloud computing giants. Retrieved November 29, 2022, from https://www.msn.com/en-us/money/companies/banks-in-eu-face-tougher-rules-on-using-cloud-computing-giants/ar-AA14E9aB

Kaushik, P., Rao, A. M., Singh, D. P., Vashisht, S., & Gupta, S. (2021). Cloud Computing and Comparison based on Service and Performance between Amazon AWS, Microsoft Azure, and Google Cloud. *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, 268–273. https://doi.org/10.1109/ICTAI53825.2021.9673425

Koninkrijksrelaties, M. v. B. Z. e. (n.d.-a). Wet op het financieel toezicht [Last Modified: 2023-01-18]. Retrieved January 23, 2023, from https://wetten.overheid.nl/BWBR0020368/2023-01-01

Koninkrijksrelaties, M. v. B. Z. e. (n.d.-b). Wet ter voorkoming van witwassen en financieren van terrorisme [Last Modified: 2023-01-18]. Retrieved January 23, 2023, from https://wetten.overheid.nl/BWBR0024282/2022-11-01

Kotas, C., Naughton, T., & Imam, N. (2018). A comparison of Amazon Web Services and Microsoft Azure cloud platforms for high performance computing [ISSN: 2158-4001]. *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 1–4. https://doi.org/10.1109/ICCE.2018.8326349

Kuiper, E. (2014). Factors Influencing the Adoption of and Business Case for Cloud Computing in the Public Sector, 10. https://www.researchgate.net/publication/277552178_Factors_Influencing_the_Adoption_of_and_Business_Case_for_Cloud_Computing_in_the_Public_Sector

Lee, J.-R., O'Neal, D. E., Pruett, M. W., & Thomas, H. (1995). Planning for dominance: A strategic perspective on the emergence of a dominant design. *R&D Management*, *25*(1), 3–15. https://doi.org/10.1111/j.1467-9310.1995.tb00896.x

Liang, F., Brunelli, M., & Rezaei, J. (2020). Consistency issues in the best worst method: Measurements and thresholds. *Omega*, *96*, 102175. https://doi.org/10.1016/j.omega.2019.102175

Maarek, S. (n.d.). Ultimate AWS Certified Cloud Practitioner - 2022. Retrieved January 25, 2023, from https://eylearning.udemy.com/course/aws-certified-cloud-practitioner-new/

Malone, T. W., Laubacher, R., & Morton, M. S. S. (2003). *Inventing the Organizations of the 21st Century* [Google-Books-ID: az_UcjtGrSgC]. MIT Press.

MarketsandMarkets. (2020). Cloud Platform Market in the Financial Services Sector. https://www.marketsandmarkets.com/PressReleases/cloud-platform.asp

Mell, P. M., & Grance, T. (2011). The NIST Definition of Cloud Computing [Last Modified: 2018-11-10T10:11-05:00 Publisher: Peter M. Mell, Timothy Grance]. *NIST*. Retrieved January 25, 2023, from https://www.nist.gov/publications/nist-definition-cloud-computing

Mitchell, T. (n.d.). AZ-900 Bootcamp: Microsoft Azure Fundamentals (JAN 2023). Retrieved January 25, 2023, from https://eylearning.udemy.com/course/az-900-azure-exam-prep-understanding-cloud-concepts/

Mitford, K. (2022). Microsoft named a Leader in 2022 Gartner® Magic Quadrant™ for Cloud Infrastructure and Platform Services. Retrieved January 10, 2023, from https://azure.microsoft.com/en-us/blog/microsoft-named-a-leader-in-2022-gartner-magic-quadrant-for-cloud-infrastructure-and-platform-services/

mobibiz. (2019). 7 Reasons That Make Cloud-Based Mobile Apps A Good Business Investment. Retrieved March 27, 2023, from https://www.mobibiz.in/blog/2019/04/22/reasons-cloud-based-mobile-apps-good-business-investment/

Morgan, L., & Conboy, K. (2013). Factors affecting the adoption of cloud computing: An exploratory study. *21st European Conference on Information Systems 2013 (ECIS)*.

Official Journal of the European Union. (2014). Markets in Financial Instruments Directive (MiFID II). Retrieved January 23, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0065&from=EN

Official Journal of the European Union. (2015). Payment Services Directive 2 (PSD2). Retrieved January 23, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366

Official Journal of the European Union. (2016). Network and Information Systems Directive (NISD). Retrieved January 23, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148

Official Journal of the European Union. (2018). EU Anti-Money Laundering Directive (AMLD). Retrieved January 23, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L0843

Official Journal of the European Union. (2019). Cybersecurity Act. Retrieved January 23, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

Official Journal of the European union. (2016). General Data Protection Regulation (GDPR). Retrieved January 23, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Opara, C. D. (2020). CLOUD COMPUTING IN AMAZON WEB SERVICES, MICROSOFT WINDOWS AZURE, GOOGLE APP ENGINE AND IBM CLOUD PLATFORMS: A COMPARATIVE STUDY, 69.

Pierleoni, P., Concetti, R., Belli, A., & Palma, L. (2020). Amazon, Google and Microsoft Solutions for IoT: Architectures and a Performance Comparison. *IEEE Access*, *8*, 5455–5470. https://doi.org/10.1109/ACCESS.2019.2961511

Rai, R., Sahoo, G., & Mehfuz, S. (2015). Exploring the factors influencing the cloud computing adoption: A systematic study on cloud migration. *SpringerPlus*, *4*(1), 197. https://doi.org/10.1186/s40064-015-0962-2

Rezaei, J. (n.d.). Best Worst Method | A multi-criteria decision-making method. Retrieved December 9, 2022, from https://bestworstmethod.com/

Rezaei, J. (2015). Best-worst multi-criteria decision-making method. *Omega*, *53*, 49–57. https://doi.org/10.1016/j.omega.2014.11.009

Rezaei, J. (2016). Best-worst multi-criteria decision-making method: Some properties and a linear model. *Omega*, *64*, 126–130. https://doi.org/10.1016/j.omega.2015.12.001

Saaty, R. W. (1987). The analytic hierarchy process—what it is and how it is used. *Mathematical Modelling*, *9*(3), 161–176. https://doi.org/10.1016/0270-0255(87)90473-8

Saaty, T. L., & Vargas, L. G. (2013). *Decision Making with the Analytic Network Process: Economic, Political, Social and Technological Applications with Benefits, Opportunities, Costs and Risks* (Vol. 195). Springer US. https://doi.org/10.1007/978-1-4614-7279-7

Sathye, M., Goundar, S., & Bhardwaj, A. (2022). Determinants of Mobile Cloud Computing Adoption by Financial Services Firms: *Journal of Information Technology Research*, *15*(1), 1–17. https://doi.org/10.4018/JITR.299921

Schilling, M. (1999). Winning the standards race:: Building installed base and the availability of complementary goods. *European Management Journal*, *17*(3), 265–274. https://doi.org/10.1016/S0263-2373(99)00005-5

Schumpeter, J. (1980). *Theory of Economic Development*. Routledge. https://doi.org/10.4324/9781315135564

Scott, H. S., Gulliver, J., & Nadler, H. (2019). Cloud Computing in the Financial Sector: A Global Perspective. Retrieved November 15, 2022, from https://papers.ssrn.com/abstract=3427220

Singh, M., Tanwar, K. S., & Srivastava, V. M. (2018). Cloud Computing Adoption Challenges in the Banking Industry. *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, 1–5. https://doi.org/10.1109/ICABCD.2018.8465412

Spiteri, A. (2020). What's cloud computing? The advantages and disadvantages. Retrieved March 27, 2023, from https://www.microsoft.com/en-gb/microsoft-365/business-insights-ideas/resources/whats-cloud-computing-the-advantages-and-disadvantages

Stewart, H. (2021). The hindrance of cloud computing acceptance within the financial sectors in Germany [Publisher: Emerald Publishing Limited]. *Information & Computer Security*, *30*(2), 206–224. https://doi.org/10.1108/ICS-01-2021-0002

Suarez, F. F. (2004). Battles for technological dominance: An integrative framework. *Research Policy*, *33*(2), 271–286. https://doi.org/10.1016/j.respol.2003.07.001

Suárez, F. F., & Utterback, J. M. (1995). Dominant designs and the survival of firms. *Strategic Management Journal*, *16*(6), 415–430. https://doi.org/10.1002/smj.4250160602

Suhr, J. (1999). *The Choosing by Advantages Decisionmaking System*. Greenwood Publishing Group.

van de Kaa, G., van den Ende, J., de Vries, H. J., & van Heck, E. (2011). Factors for winning interface format battles: A review and synthesis of the literature. *Technological Forecasting and Social Change*, *78*(8), 1397–1411. https://doi.org/10.1016/j.techfore.2011.03.011

Vries, H. J. d. (2013). *Standardization: A Business Approach to the Role of National Standardization Organizations* [Google-Books-ID: avPiBwAAQBAJ]. Springer Science & Business Media.

Wankhede, P., Talati, M., & Chinchamalatpure, R. (2020). COMPARATIVE STUDY OF CLOUD PLATFORMS -MICROSOFT AZURE, GOOGLE CLOUD PLATFORM AND AMAZON EC2. *Journal of Research in Engineering and Applied Sciences*, *05*(02), 60–64. https://doi.org/10.46565/jreas.2020.v05i02.004

Werth, O., Schwarzbach, C., Rodríguez Cardona, D., Breitner, M. H., & Graf von der Schulenburg, J.-M. (2020). Influencing factors for the digital transformation in the financial services sector. *Zeitschrift für die gesamte Versicherungswissenschaft*, *109*(2-4), 155–179. https://doi.org/10.1007/s12297-020-00486-6

A

Interviews

In this appendix the setup and results are presented per interview round.

A.1. Round 1

A.1.1. Setup

Interviewees

- I1 2023: Manager FSO Technology Transformation in consulting (Netherlands). January 13th 2023 via a Teams
- I2 2023: Senior Manager FSO Data & Analytics in consulting (Netherlands). January 13th 2023 at the office
- I3 2023: Senior Consultant FSO Technology Transformation in consulting (Netherlands). January 19th 2023 via Teams

Questions
Introduction of Thesis topic, goals and structure of this interview

General part

1. Am I allowed to record this interview?
2. What is your function?
3. At what organisation(s) do (did) you work?
4. What is your work experience related to Cloud?
5. With which Cloud platform(s) do (did) you work?

Core concepts Cloud

1. Can you name some important events that led to Cloud as we know today?
2. Did the Cloud originally had a different application before the Cloud we know today?
3. What major changes have taken place in the past and what were the differences between the previous form and the new form?
4. What do you foresee as the future of cloud?

Market characteristics

1. What were your expectations before the battle between cloud platforms started?
2. What was the final result in the Dutch financial sector?

   (a) What are commonly used Cloud platforms (AWS, Azure, Google Cloud)
   (b) What are commonly used Cloud Service Models (IaaS, PaaS, SaaS, (XaaS))

(c) What are commonly used Cloud Deployment Models (Public, Private, Community, Hybrid)

3. Did the winning parties had a special strategy for winning the battle?
4. Why is (was) this strategy so (un)successful?
5. Why is it that the competing platforms lost the battle?
6. Were there any turns by the development of the platforms that determined failure or success?
7. Did the final result that you expected come true? Why (not)?
8. What do you expect for the future in this sector?

IT regulations and impact on Cloud adoption

1. Can you name specific IT regulations in the financial sector related to Cloud?
2. What are the most important one's?
3. How do these regulations affect the adoption of Cloud?
4. What are the biggest challenges for Cloud related to comply with the regulation?

Factors for Cloud adoption

1. What was, according to you, the most relevant factor for the outcome of the battle?
2. Which factors played a role in the battle? What were, according to you, the success or fail factors?
3. Which factors (that had an influence on becoming a dominant platform) were known from the beginning?
4. I present a list of 29 factors; can you explain the relevance of each factor within this battle?
5. In your opinion, are there any factors which should be added to the list of 29 factors because they would be decisive success factors in a specific case or factors for failure?

End

1. Do you have sources concerning this platform battle that could be useful for this study?
2. May I contact you in the future after processing the interview by phone, email or otherwise and present the results of the interview to correct misinterpretations or other details?
3. Do you know any other individuals within your network who you think I should talk to?

Thank you for your time!

A.1.2. Results

The table with the factor count can be found in Appendix B. Furthermore, the summaries of the interview transcripts can be accessed upon request from the author of this paper.

A.2. Round 2

A.2.1. Setup

Interviewees

- I1 2023: Manager FSO Technology Transformation in consulting (Netherlands). February 20th 2023 on the office
- I2 2023: Senior Manager FSO Data & Analytics in consulting (Netherlands). February 20th 2023 on the office
- I3 2023: Senior Consultant FSO Technology Transformation in consulting (Netherlands). February 24th 2023 via Teams
- I4 2023: Manager Cybersecurity FSO Technology Transformation in consulting (Netherlands). February 27th 2023 via a Teams
- I5 2023: Customer Director in consulting (Netherlands). February 22th 2023 on their office
- I6 2023: Product Owner Cloud (Banking) in consulting. February 23th 2023 via Teams

- I7 2023: Security Analyst/Architect/Engineer in insurance (Netherlands). February 21th 2023 via Teams
- I8 2023: Manager IT in insurance (Netherlands). March 1st 2023 via Teams
- I9 2023: IT-Architect in insurance (Netherlands). February 27th 2023 via Teams
- I10 2023: Product Owner Cloud in banking (Netherlands). February 21st 2023 via Teams
- I11 2023: Solution Architect in banking (Netherlands). March 7th 2023 via Teams
- I12 2023: Product Owner data and reporting in regulator (Netherlands). February 21th 2023 on their office
- I13 2023: Associate Professor TPM, Head ICT section in academic (Netherlands). February 22th 2023 via Teams

Questions
Introduction of Thesis topic, goals and structure of this interview

General part

1. Am I allowed to record this interview?
2. What is your function?
3. At what organisation(s) do (did) you work?
4. What is your work experience related to Cloud?
5. With which Cloud platform(s) do (did) you work?

BWM - Factors Introduction and explanation factors and method

1. Could you please grab the list of factors and definitions?
2. Do you understand all the factors and their categories or still have questions?

For each category:

1. What is for the adoption of a Cloud platform within the Dutch Financial sector the most important factor within this category?
2. What is for the adoption of a Cloud platform within the Dutch Financial sector the least important factor within this category?
3. Can you please express your preference on ”the most important factor over all the other factors” by selecting a number between 1 and 9 from the drop-box?
4. Can you please express your preference on ”all the other factors over the least important factor” by selecting a number between 1 and 9 from the drop-box?

BWM - Platform comparison Introduction and explanation platforms and method
For each factor

1. What platform scores best on this factor in the Dutch Financial sector?
2. What platform scores worst on this factor in the Dutch Financial sector?
3. Can you please express your preference on “the Best platform over all the other platform” by selecting a number between 1 and 9 from the drop-box?
4. Can you please express your preference on “all the other platform over the Worst platform” by selecting a number between 1 and 9 from the drop-box?

End

1. Do you have sources concerning this platform battle that could be useful for this study?
2. May I contact you in the future after processing the interview by phone, email or otherwise and present the results of the interview to correct misinterpretations or other details?

Thank you for your time!

A.2.2. Results

The results of the BWM factor section can be found in Appendix C. In addition, the results of the BWM platform comparison section can be found in Appendix D. Furthermore, summaries of the interview transcripts are available from the author of this paper upon request.

A.3. Round 3

A.3.1. Setup

Interviewees

- I1 2023: Product Owner Cloud in banking (Netherlands). March 15th 2023 via Teams
- I2 2023: Solution Architect in banking (Netherlands). March 15th 2023 via Teams
- I3 2023: IT-Architect in insurance (Netherlands). March 16th 2023 via Teams

Questions

Introduction of Thesis topic, goals and structure of this interview

General part

1. Am I allowed to record this interview?
2. What is your function?
3. At what organisation(s) do (did) you work?
4. What is your work experience related to Cloud?
5. With which Cloud platform(s) do (did) you work?

Validation Factors Show BWM factor results

1. Do you understand all the factors and their categories or still have questions?

For category weights:

1. How can you explain the ranking?
2. Why does number 1 emerge as the most important?
3. Why does number 5 come out as least important?

For global weights:

1. Why do you think the top 5 is more important than the others?
2. Why do you think the last 5 are less important than the others?
3. Do you have any other comments or comments about the ranking of the factors?

Validation platform comparison Show BWM platform comparison results

1. How can you explain the ranking?
2. Why does number 1 emerge as the most important?
3. Why does number 3 emerge as least important?
4. Any other comments?

Thank you for your time!

A.3.2. Results

The summaries of the interview transcripts are available from the author of this paper upon request.

B

Relevant factors

B.1. Cloud adoption articles

Table B.1: Cloud adoption articles part 1

#	Title	Author(s)	Year
1	Why Cloud? - A Review of Cloud Adoption Determinants in Organizations	Asatiani	2015
2	Factors affecting the adoption of cloud services in enterprises	Hsu & Lin	2016
3	Customers perspectives on adoption of cloud computing in banking sector	Asadi et al.	2017
4	Factors affecting the adoption of cloud computing: An exploratory study	Morgan & Conboy	2013
5	Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration	Rai et al.	2015
6	Influencing factors for the digital transformation in the financial services sector	Werth et al.	2020
7	Determinants of Mobile Cloud Computing Adoption by Financial Services Firms	Sathye et al.	2022
8	An empirical study on effective factors on adoption of cloud computing in electronic banking: a case study of Iran banking sector	Alizadeh et al.	2020
9	Cloud-Computing in Banking Influential Factors, Benefits and Risks from a Decision Maker's Perspective	Rieger et al.	2013
10	Understanding determinants of cloud computing adoption using an integrated TAM-TOE model	Gangwar et al.	2014
11	A View on Cloud Computing in the Banking Sector	Sudhakar et al.	2014
12	Adoption of Cloud Computing model for Managing e-Banking System in Banking Organizations	Elzamy et al.	2019
13	FINANCIAL DATA SECURITY IN CLOUD COMPUTING	Hariharan	2021
14	Adoption Issues for Cloud Computing	Kim et al.	2009
15	Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding return on investment.	Misra & Mondal	2011
16	Cloud computing for education: A new dawn?	Sultan	2010
17	Challenges and Benefits for Adopting the Paradigm of Cloud Computing	Brohi & Bamiah	2011

Table B.2: Cloud adoption articles part 2

#	Title	Author(s)	Year
18	Developing an explorative model for SaaS adoption	Wu	2011
19	SECURITY ISSUES OF BANKING ADOPTING THE APPLICATION OF CLOUD COMPUTING	Rani & Gangal	2012
20	Factors Affecting Cloud Technology Adoption: Potential User's Perspective	Ogunde & Mehnen	2013
21	Privacy, Security and Trust in Cloud Computing	Pearson	2012
22	Cloud Computing Adoption Journey within Organizations	Swamy	2013
23	The usage and adoption of cloud computing by small and medium businesses	Gupta et al.	2013
24	The role of trust and risk perceptions in cloud archiving — Results from an empirical study	Burda & Teuteberg	2014
25	Impacts on the organizational adoption of cloud computing: A reconceptualization of influencing factors	Stieninger et al.	2014
26	Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors	Oliveira et al.	2014

B.2. Final factor count

Table B.3: Final factor count in articles part 1

#	Factors	Interview			Articles																										
Firm level factors		**1**	**2**	**3**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**Total (#)**	**Total (%)**
Characteristics of the format supporter																															
1	Financial strength	x	x	x					x			x	x		x	x							x								9	31,0
2	Brand reputation and credibility	x	x	x	x								x		x	x							x					x			9	31,0
3	Operational supremacy	x	x	x	x	x			x	x		x				x							x								10	34,5
4	Learning orientation	x	x	x	x		x			x			x			x							x								9	31,0
5	Location of data				x								x		x								x								4	13,8
6	Customer support				x																										1	3,5
Characteristics of the format																															
7	Technological superiority	x	x	x	x	x		x		x	x	x	x	x				x		x	x							x	x	x	17	58,6
8	Compatibility	x	x	x		x		x	x		x	x		x		x		x			x		x						x	x	15	51,7
9	Complementary goods		x	x						x																					3	10,3
10	Flexibility	x	x	x	x					x						x			x												7	24,1
11	Scalability				x	x		x	x							x			x		x										7	24,1
12	Complexity				x	x		x	x		x	x		x															x		8	27,6
13	Security & Privacy				x	x	x	x	x		x	x	x			x	x	x		x	x	x	x	x	x	x	x		x	x	21	72,4
14	Availability				x							x				x		x		x	x		x	x	x		x				10	34,5
15	Trialability					x		x																							2	6,9
16	Recovery														x								x								2	6,9
17	Implementation times				x			x																							2	6,9

Table B.4: Final factor count in articles part 2

#	Factors	Interview			Articles																											
Firm level factors		**1**	**2**	**3**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**Total (#)**	**Total (%)**
Format support strategy																																
18	Pricing strategy	x	x	x	x	x	x	x	x	x	x	x	x				x	x	x	x	x	x		x		x	x		x	x	23	79,3
19	Pre-emption of scarce assets			x																												1	3,5
20	Appropriability strategy			x																												1	3,5
21	Timing of entry	x	x	x						x																						4	13,8
22	Marketing Communications	x	x	x																												3	10,3
23	Distribution strategy	x	x	x																												3	10,3
24	Commitment	x	x	x	x				x		x	x	x	x																	x	10	34,5
Other stakeholders																																
25	Current installed base	x	x	x	x																											4	13,8
26	Previous installed base			x																												1	3,5
27	Big Fish		x	x	x																											3	10,3
28	Antitrust laws	x		x																												2	6,9
29	Suppliers	x		x						x																						3	10,3
30	Effectiveness of the format development process	x		x																												2	6,9
31	Network of stakeholders	x	x	x	x				x																							5	17,2
32	Regulator	x		x	x	x		x	x	x	x	x	x		x	x		x					x	x	x	x				x	18	62,1
Environmental factors																																
Market characteristics																																
33	Bandwagon effect		x	x	x	x				x			x	x																x	8	27,6
34	Network externalities	x		x	x						x					x															5	17,2
35	Number of options available	x		x								x																				3	10,3
36	Uncertainty in the market		x	x	x					x																						4	13,8
37	Rate of change	x	x		x	x						x																				5	17,2
38	Switching costs	x	x	x	x	x						x				x	x							x								9	31,0
39	Cultural barriers												x																			1	3,5

C

BWM factors

Table C.1: Complete results BWM factors Part 1

#	Factors	Interview													Local Average Weight	Average Global Weight	Global ranking
		1	2	3	4	5	6	7	8	9	10	11	12	13			
Firm level factors																	
Characteristics of the Cloud provider		0,4907	0,3120	0,1963	0,1809	0,1235	0,0470	0,0455	0,3176	0,0916	0,4019	0,4167	0,1244	0,5315	**0,2278**		
1	Financial strength	0,1840	0,0541	0,3176	0,1235	0,0592	0,1577	0,0392	0,1194	0,0533	0,0762	0,2625	0,0600	0,1132	0,1274	0,0290	**14**
2	Brand reputation and credibility	0,4455	0,5405	0,1765	0,4165	0,0995	0,4158	0,1961	0,1194	0,0844	0,4406	0,1313	0,1600	0,2830	0,2821	0,0642	**2**
3	Operational supremacy	0,1840	0,2162	0,3176	0,2470	0,1659	0,1183	0,0980	0,0585	0,4400	0,2667	0,0477	0,2400	0,1132	0,2032	0,0463	**8**
4	Location of data	0,1380	0,0811	0,0706	0,0484	0,4265	0,2366	0,1961	0,5035	0,1689	0,0387	0,4535	0,1200	0,4528	0,2054	0,0468	**7**
5	Learning orientation	0,0484	0,1081	0,1176	0,1646	0,2488	0,0717	0,4706	0,1991	0,2533	0,1778	0,1050	0,4200	0,0377	0,1819	0,0414	**10**
Characteristics of the Cloud Platform		0,1869	0,3120	0,3645	0,4651	0,2470	0,5359	0,4545	0,1765	0,2290	0,2336	0,2500	0,0697	0,2067	**0,3046**		
6	Technological superiority	0,1220	0,1467	0,0851	0,1992	0,0401	0,0517	0,2793	0,0370	0,0359	0,1139	0,0281	0,0642	0,0405	0,0919	0,0249	**19**
7	Compatibility	0,3049	0,2201	0,1277	0,3321	0,0868	0,2069	0,1117	0,1323	0,1149	0,1709	0,1311	0,1070	0,1336	0,1709	0,0520	**5**
8	Complementary goods	0,0305	0,0550	0,0638	0,0996	0,0868	0,0300	0,1676	0,0794	0,1724	0,0244	0,0787	0,0802	0,0668	0,0753	0,0229	**22**
9	Flexibility	0,0915	0,0550	0,0638	0,0797	0,0651	0,0690	0,0670	0,0794	0,0690	0,0854	0,0655	0,1604	0,0668	0,0835	0,0254	**18**
10	Scalability	0,0732	0,0734	0,2128	0,0664	0,1302	0,1379	0,0279	0,0661	0,0690	0,0854	0,0787	0,1070	0,1336	0,0966	0,0294	**13**
11	Complexity	0,0732	0,0629	0,0213	0,0332	0,1302	0,0591	0,0670	0,0794	0,0862	0,0683	0,0983	0,0401	0,0891	0,0704	0,0215	**24**
12	Security & Privacy	0,1829	0,3535	0,2128	0,1328	0,2304	0,3419	0,1676	0,3280	0,2802	0,2807	0,1966	0,2807	0,2348	0,2643	0,0805	**1**

Table C.2: Complete results BWM factors Part 2

#	Factors	Interview													Local Average Weight	Average Global Weight	Global ranking
		1	2	3	4	5	6	7	8	9	10	11	12	13			
Firm level factors																	
13	Availability	0,1220	0,0333	0,2128	0,0569	0,2304	0,1035	0,1117	0,1984	0,1724	0,1709	0,3230	0,1604	0,2348	0,1571	0,0479	**6**
Cloud provider support strategy		0,0701	0,1680	0,1963	0,0646	0,1646	0,2163	0,1818	0,3176	0,1527	0,2336	0,1667	0,0995	0,0886	**0,1759**		
14	Pricing strategy	0,4343	0,2276	0,2816	0,2532	0,2273	0,4774	0,1026	0,4824	0,4565	0,2588	0,1687	0,2338	0,2117	0,3109	0,0547	**3**
15	Timing of entry	0,0505	0,4000	0,1068	0,4270	0,3864	0,0491	0,0462	0,1122	0,0652	0,1035	0,1265	0,1169	0,0460	0,1293	0,0228	**23**
16	Marketing Communications	0,0859	0,0690	0,0485	0,1013	0,1136	0,1123	0,1538	0,0449	0,1739	0,0375	0,0361	0,0649	0,1270	0,0920	0,0162	**28**
17	Distribution strategy	0,1717	0,1517	0,2816	0,0497	0,0455	0,0802	0,4923	0,0801	0,1739	0,1725	0,2530	0,1558	0,0907	0,1580	0,0278	**17**
18	Commitment	0,2576	0,1517	0,2816	0,1688	0,2273	0,2808	0,2051	0,2804	0,1304	0,4276	0,4157	0,4286	0,5246	0,3098	0,0545	**4**
Other stakeholders		0,1402	0,0960	0,1121	0,1085	0,0484	0,1081	0,1818	0,0706	0,4122	0,0374	0,0417	0,2488	0,0492	**0,1177**		
19	Current installed base	0,1878	0,2404	0,2143	0,1183	0,2378	0,2679	0,0482	0,1356	0,1672	0,4406	0,2000	0,1238	0,1282	0,2020	0,0238	**21**
20	Big Fish	0,1878	0,2404	0,0536	0,0717	0,1189	0,0893	0,0783	0,1130	0,1672	0,0387	0,0500	0,2476	0,1026	0,1204	0,0142	**29**
21	Regulator	0,4751	0,0437	0,3750	0,4158	0,4299	0,4554	0,4036	0,5378	0,1254	0,2667	0,3500	0,4476	0,4487	0,3730	0,0439	**9**
22	Suppliers	0,0552	0,0601	0,2143	0,1577	0,0549	0,1339	0,2349	0,1694	0,4759	0,1778	0,2000	0,0571	0,2564	0,1652	0,0194	**25**
23	Network of stakeholders	0,0939	0,4153	0,1429	0,2366	0,1585	0,0536	0,2349	0,0442	0,0643	0,0762	0,2000	0,1238	0,0641	0,1395	0,0164	**27**
Environmental factors																	
Market characteristics		0,1121	0,1120	0,1308	0,1809	0,4165	0,0927	0,1364	0,1176	0,1145	0,0935	0,1250	0,4577	0,1240	**0,1740**		
24	Bandwagon effect	0,0641	0,2268	0,0425	0,1498	0,1950	0,1244	0,1282	0,0652	0,2326	0,0804	0,0371	0,0386	0,0375	0,1102	0,0192	**26**
25	Network externalities	0,1058	0,0412	0,0867	0,2248	0,1950	0,0711	0,1282	0,0942	0,4070	0,1286	0,2340	0,1202	0,1725	0,1651	0,0287	**15**
26	Number of options available	0,1058	0,0567	0,3653	0,0899	0,3428	0,0415	0,1026	0,0942	0,0930	0,0474	0,1560	0,2961	0,1035	0,1432	0,0249	**20**
27	Uncertainty in the market	0,1410	0,2268	0,1444	0,1124	0,0591	0,0995	0,0534	0,5109	0,1163	0,0804	0,4012	0,0901	0,0863	0,1601	0,0279	**16**
28	Rate of change	0,3718	0,0567	0,1444	0,0441	0,1300	0,4147	0,4167	0,1413	0,0581	0,5347	0,0780	0,3348	0,1725	0,2048	0,0356	**12**
29	Switching costs	0,2115	0,3918	0,2167	0,3790	0,0780	0,2488	0,1709	0,0942	0,0930	0,1286	0,0936	0,1202	0,4276	0,2165	0,0377	**11**

D

BWM Platform comparison

D.1. Consistency Ratio's

Table D.1: Complete results Consistency Ratio's Platform Comparison part 1

		Expert												
#	**Factors**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Firm level factors														
Characteristics of the Cloud provider														
1	Financial strength	0,1667		0,0500	0,1667	0,1333	0,0000			0,0500	0,0667	0,1667	0,1667	
2	Brand reputation and credibility	0,0500	0,0667	0,1667	0,0000	0,1333	0,0000	0,0667	0,0972	0,1000		0,1000	0,0000	0,0000
3	Operational supremacy	0,1667	0,0000	0,1667	0,1667	0,0000	0,0500			0,0500				
4	Location of data	0,0000	0,0000	0,0000	0,0000	0,1667	0,0000	0,0000		0,1667		0,0000		
5	Learning orientation	0,0833	0,1667	0,0000	0,1667		0,0000			0,1667			0,0000	
Characteristics of the Cloud Platform														
6	Technological superiority	0,0000		0,0000	0,5000	0,1667	0,0500			0,0500	0,0000		0,0000	
7	Compatibility	0,0833	0,0000	0,1667	0,1667		0,0000		0,0833	0,0500	0,1000	0,0667	0,0000	
8	Complementary goods	0,0000		0,0000	0,1667	0,1000	0,0500	0,0667		0,0500	0,0500	0,0500	0,1667	0,0000
9	Flexibility	0,0000	0,1667	0,1667	0,0000					0,0500	0,0000			
10	Scalability	0,0000		0,1667	0,0000		0,0000		0,0000	0,0500	0,0000	0,0000		
11	Complexity	0,0500			0,1667		0,0000			0,0500	0,0000		0,1667	
12	Security & Privacy	0,0000	0,0000		0,0000		0,0000	0,0500	0,1528		0,0500	0,0000		
13	Availability	0,1667			0,0000		0,0000		0,0000		0,0000			
Cloud provider support strategy														
14	Pricing strategy	0,0000	0,0000	0,0000			0,0000			0,1190				
15	Timing of entry	0,0000	0,0667	0,0000	0,0500	0,1000	0,1000	0,1190		0,0000	0,1667			
15	Marketing Communications	0,0000		0,0000			0,0000	0,0714	0,0000	0,0500				
17	Distribution strategy	0,0500	0,1667	0,0000	0,1667	0,0500	0,0000	0,1190		0,0000	0,0500	0,0000	0,0000	
18	Commitment	0,0000	0,0000	0,0000	0,0000		0,0000			0,0500		0,0000		
Other stakeholders														
19	Current installed base	0,1071	0,0500	0,0000	0,0667	0,0476	0,0179	0,1250		0,0000	0,0500	0,0500	0,1667	
20	Big Fish	0,1667			0,0000		0,0000		0,1250					
21	Regulator	1,0000			0,1667				0,1250		0,0500	0,1190		0,0000
22	Suppliers	0,0000		0,0000	0,1667		0,0000	0,0500		0,1667	0,0500		0,0000	
23	Network of stakeholders	0,1667	0,0714		0,0500		0,0000	0,0500	0,1250			0,0667	0,0000	

Table D.2: Complete results Consistency Ratio's Platform Comparison part 2

		Expert												
#	**Factors**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Environmental factors														
Market characteristics														
24	Bandwagon effect	0,0000			0,0000		0,1667	0,0667	0,0000	0,1667	0,0500			
25	Network externalities	0,0000		0,1667	0,1667	0,0000	0,0000		0,0000		0,0500		0,1667	
26	Number of options available	0,0000			0,0000		0,0000		0,0000		0,0500			
27	Uncertainty in the market	0,0000	0,0000		0,0000	0,0000	0,0000		0,0500					
28	Rate of change	0,0000		0,0000	0,0000	0,0500	0,0000	0,0476	0,0000	0,0000	0,0000	0,0000		
29	Switching costs	0,0000			0,1667		0,0000		0,1071		0,0000	0,0000		

D.2. Complete results BWM platform comparison

Table D.3: Complete results BWM platform comparison part 1

Factors / Firm level factors	Cloud Platform	1	2	3	4	5	6	7	8	9	10	11	12	13	Local Average Weight
Characteristics of the Cloud provider															
Financial strength	AWS	0,2917		0,2250	0,2917	0,3333	0,3333			0,6500		0,2917	0,5417		**0,3708**
	Azure	0,5417		0,6500	0,5417	0,5833	0,3333			0,2250		0,5417	0,2917		**0,4642**
	Google	0,1667		0,1250	0,1667	0,0833	0,3333			0,1250		0,1667	0,1667		**0,1650**
Brand reputation and credibility	AWS	0,6500	0,1852	0,1667	0,4286	0,5833	0,4286	0,3182	0,3472	0,6600	0,1111	0,2400	0,4000	0,4545	**0,3782**
	Azure	0,2250	0,7037	0,5417	0,4286	0,3333	0,4286	0,5909	0,5972	0,1000	0,7037	0,6600	0,4000	0,4545	**0,4773**
	Google	0,1250	0,1111	0,2917	0,1429	0,0833	0,1429	0,0909	0,0556	0,2400	0,1852	0,1000	0,2000	0,0909	**0,1445**
Operational supremacy	AWS	0,2917	0,3333	0,1667	0,5417	0,1429	0,5833			0,2250					**0,3118**
	Azure	0,5417	0,3333	0,5417	0,2917	0,5714	0,3056			0,6500					**0,4772**
	Google	0,1667	0,3333	0,2917	0,1667	0,2857	0,1111			0,1250					**0,2110**
Location of data	AWS	0,3333	0,3333	0,4000	0,3333	0,2917	0,3333	0,2857		0,2917		0,1250			**0,3059**
	Azure	0,3333	0,3333	0,4000	0,3333	0,5417	0,3333	0,5714		0,5417		0,7500			**0,4626**
	Google	0,3333	0,3333	0,2000	0,3333	0,1667	0,3333	0,1429		0,1667		0,1250			**0,2315**
Learning orientation	AWS	0,4583	0,2917	0,3333	0,5417		0,3333			0,2917			0,2500		**0,3641**
	Azure	0,4167	0,5417	0,3333	0,1667		0,3333			0,5417			0,5000		**0,4000**
	Google	0,1250	0,1667	0,3333	0,2917		0,3333			0,1667			0,2500		**0,2359**
Characteristics of the Cloud Platform															
Technological superiority	AWS	0,4286		0,1429	0,5625	0,5417	0,5833			0,1250	0,3333		0,2500		**0,3528**
	Azure	0,4286		0,5714	0,1875	0,2917	0,3056			0,6500	0,3333		0,5000		**0,4184**
	Google	0,1429		0,2857	0,2500	0,1667	0,1111			0,2250	0,3333		0,2500		**0,2288**
Compatibility	AWS	0,4118	0,1667	0,5417	0,2917		0,3333		0,1648	0,3056	0,2400	0,0909	0,2500		**0,2693**
	Azure	0,4706	0,6667	0,2917	0,5417		0,3333		0,7582	0,5833	0,6600	0,5909	0,5000		**0,5571**
	Google	0,1176	0,1667	0,1667	0,1667		0,3333		0,0769	0,1111	0,1000	0,3182	0,2500		**0,1736**
Complementary goods	AWS	0,1429		0,1429	0,1667	0,1000	0,5833	0,3182		0,3056	0,1250	0,2250	0,2917	0,3333	**0,2329**
	Azure	0,5714		0,5714	0,5417	0,6600	0,3056	0,5909		0,5833	0,6500	0,6500	0,5417	0,3333	**0,5669**
	Google	0,2857		0,2857	0,2917	0,2400	0,1111	0,0909		0,1111	0,2250	0,1250	0,1667	0,3333	**0,2002**
Flexibility	AWS	0,3333	0,1667	0,1667	0,3333					0,5833	0,3333				**0,3120**
	Azure	0,3333	0,5417	0,5417	0,3333					0,1111	0,3333				**0,3505**
	Google	0,3333	0,2917	0,2917	0,3333					0,3056	0,3333				**0,3375**

Table D.4: Complete results BWM platform comparison part 2

Factors / **Firm level factors**	**Cloud Platform**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**Local Average Weight**
Characteristics of the Cloud platform															
Scalability	AWS	0,3333		0,1667	0,3333		0,3333		0,3333	0,6500	0,3333	0,3333			**0,3470**
	Azure	0,3333		0,5417	0,3333		0,3333		0,3333	0,1250	0,3333	0,3333			**0,3272**
	Google	0,3333		0,2917	0,3333		0,3333		0,3333	0,2250	0,3333	0,3333			**0,3259**
Complexity	AWS	0,1250			0,2917		0,3333			0,5938	0,3333		0,5417		**0,3658**
	Azure	0,2250			0,5417		0,3333			0,2813	0,3333		0,2917		**0,3562**
	Google	0,6500			0,1667		0,3333			0,1250	0,3333		0,1667		**0,2780**
Security & Privacy	AWS	0,4615	0,2500		0,2857		0,4000	0,3056	0,2111		0,2250	0,3333			**0,3132**
	Azure	0,4615	0,5000		0,5714		0,4000	0,5833	0,7222		0,6500	0,3333			**0,5376**
	Google	0,0769	0,2500		0,1429		0,2000	0,1111	0,0667		0,1250	0,3333			**0,1492**
Availability	AWS	0,1538			0,3333		0,3333		0,3333		0,3333				**0,2901**
	Azure	0,3846			0,3333		0,3333		0,3333		0,3333				**0,3485**
	Google	0,4615			0,3333		0,3333		0,3333		0,3333				**0,3614**
Cloud provider support strategy															
Pricing strategy	AWS	0,1429	0,2000	0,4286			0,3333			0,6667	0,5417				**0,3866**
	Azure	0,2857	0,2000	0,4286			0,3333			0,2500	0,1667				**0,3028**
	Google	0,5714	0,6000	0,1429			0,3333			0,0833	0,2917				**0,3106**
Timing of entry	AWS	0,4545	0,7037	0,4000	0,5833	0,6600	0,6600	0,7121		0,4667					**0,5885**
	Azure	0,4545	0,1852	0,4000	0,3056	0,2400	0,2400	0,1970		0,4667					**0,3038**
	Google	0,0909	0,1111	0,2000	0,1111	0,1000	0,1000	0,0909		0,0667					**0,1077**
Marketing Communications	AWS	0,4615		0,1429			0,4000	0,3269	0,3333	0,1250					**0,2911**
	Azure	0,4615		0,4286			0,4000	0,5962	0,3333	0,6500					**0,5086**
	Google	0,0769		0,4286			0,2000	0,0769	0,3333	0,2250					**0,2002**
Distribution strategy	AWS	0,3056	0,2917	0,2500	0,5417	0,3056		0,1970		0,2500	0,1250	0,1667	0,2500		**0,2610**
	Azure	0,5833	0,5417	0,5000	0,2917	0,5833		0,7121		0,5000	0,6500	0,6667	0,5000		**0,5632**
	Google	0,1111	0,1667	0,2500	0,1667	0,1111		0,0909		0,2500	0,2250	0,1667	0,2500		**0,1759**
Commitment	AWS	0,4444	0,4286	0,3333	0,4286		0,3333			0,1111		0,3333			**0,3379**
	Azure	0,4444	0,4286	0,3333	0,4286		0,3333			0,5833		0,3333			**0,4282**
	Google	0,1111	0,1429	0,3333	0,1429		0,3333			0,3056		0,3333			**0,2340**

Table D.5: Complete results BWM platform comparison part 3

Factors Firm level factors	Cloud Platform	1	2	3	4	5	6	7	8	9	10	11	12	13	Local Average Weight
Other stakeholders															
Current installed base	AWS	0,5938	0,2250	0,1429	0,3182	0,6727	0,6833	0,1667		0,4286	0,2250	0,3056	0,5417		**0,1779**
	Azure	0,3438	0,6500	0,5714	0,5909	0,2364	0,2333	0,7500		0,4286	0,6500	0,5833	0,2917		**0,4960**
	Google	0,0625	0,1250	0,2857	0,0909	0,0909	0,0833	0,0833		0,1429	0,1250	0,1111	0,1667		**0,1261**
Big Fish	AWS	0,2917			0,3333		0,3333		0,2625						**0,3241**
	Azure	0,5417			0,3333		0,3333		0,6750						**0,4791**
	Google	0,1667			0,3333		0,3333		0,0625						**0,1968**
Regulator	AWS	0,3000			0,2917				0,2625		0,2250	0,2500		0,4545	**0,2965**
	Azure	0,5000			0,5417				0,6750		0,6500	0,6667		0,4545	**0,5888**
	Google	0,2000			0,1667				0,0625		0,1250	0,0833		0,0909	**0,1147**
Suppliers	AWS	0,1429		0,1429	0,5417		0,4286	0,2813		0,2917	0,2250		0,2500		**0,2752**
	Azure	0,5714		0,5714	0,2917		0,4286	0,5938		0,5417	0,6500		0,5000		**0,5321**
	Google	0,2857		0,2857	0,1667		0,1429	0,1250		0,1667	0,1250		0,2500		**0,1927**
Network of stakeholders	AWS	0,1667	0,1944		0,2250		0,4286	0,2250	0,2625			0,1852	0,4000		**0,2572**
	Azure	0,5417	0,7222		0,6500		0,4286	0,6500	0,6750			0,7037	0,4000		**0,6086**
	Google	0,2917	0,0833		0,1250		0,1429	0,1250	0,0625			0,1111	0,2000		**0,1342**
Environmental															
Market characteristics															
Bandwagon effect	AWS	0,3333			0,3333		0,5417	0,1852	0,3333	0,2917	0,3056				**0,3384**
	Azure	0,3333			0,3333		0,2917	0,7037	0,3333	0,5417	0,5833				**0,4492**
	Google	0,3333			0,3333		0,1667	0,1111	0,3333	0,1667	0,1111				**0,2124**
Network externalities	AWS	0,4545		0,1667	0,2917	0,3333	0,3333		0,4615		0,3056		0,5417		**0,3632**
	Azure	0,4545		0,5417	0,5417	0,3333	0,3333		0,4615		0,5833		0,2917		**0,4563**
	Google	0,0909		0,2917	0,1667	0,3333	0,3333		0,0769		0,1111		0,1667		**0,1805**
Number of options available	AWS	0,3333					0,3333		0,4545		0,1111				**0,2963**
	Azure	0,3333					0,3333		0,4545		0,5833				**0,4485**
	Google	0,3333					0,3333		0,0909		0,3056				**0,2552**
Uncertainty in the market	AWS	0,3333	0,4444		0,4286	0,4706	0,3333		0,3056						**0,3986**
	Azure	0,3333	0,4444		0,4286	0,4706	0,3333		0,5833						**0,4440**
	Google	0,3333	0,1111		0,1429	0,0588	0,3333		0,1111						**0,1574**
Rate of change	AWS	0,3333		0,2500	0,3333	0,1250	0,5714	0,0909	0,2857	0,4286	0,3333	0,3333			**0,3036**
	Azure	0,3333		0,5000	0,3333	0,6500	0,2857	0,2364	0,1429	0,4286	0,3333	0,3333			**0,3676**
	Google	0,3333		0,2500	0,3333	0,2250	0,1429	0,6727	0,5714	0,1429	0,3333	0,3333			**0,3288**
Switching costs	AWS	0,2000			0,5417		0,3333		0,5938		0,3333	0,3333			**0,3916**
	Azure	0,2000			0,1667		0,3333		0,0625		0,3333	0,3333			**0,2211**
	Google	0,6000			0,2917		0,3333		0,3438		0,3333	0,3333			**0,3873**