DELFT UNIVERSITY

MASTER THESIS

The Dutch Public Sector and Cloud Computing

Motivating factors in the decision-making process and their interaction

Supervisors:
First Supervisor and Chair: Prof. Dr. Ir. Nitesh Bharosa
Second Supervisor: Dr. Geerten van de Kaa
External Supervisor: Gina Plat
Advisor: Dr. Jacobien Oosterhoff

Author:
Marleen van Merrienboer
5653835

Master Management of Technology

15 September 2023

Executive Summary

Technology advancements and growing demands from citizens brought about a digital transformation of the Dutch public sector. As the digital standard rises higher and higher, the Dutch public sector is faced with the task to offer a strong digital environment and can choose to do so by either maintaining current IT infrastructures or by investing in alternatives.

At the moment the most promising alternative seems to be cloud technology. Cloud technology, or more specifically public cloud technology, provides the option to 'rent' computing resources remotely from an external party. It is already widely in use within the private sector, as well as in some European governments. However, to introduce public cloud technology some hurdles must be overcome, such as concerns related to data security or the dependence on soft- and hardware that has been superseded but is difficult to replace. To gain more insight into the issue of the public cloud being a viable option to accommodate future digital transformation, it is first and foremost important to know what variables play a role in the decision-making process: what are the incentives to answer this question with either a 'yes' or a 'no'? The objective of this study will therefore be to investigate this landscape of variables that influence the decision to adopt public cloud technology. It starts with the identification of variables from current research and reports, and then explores possible interrelationships. The identification and classification of these relationships could eventually help to bring about a well-considered decision about public cloud adoption in the Dutch public sector.

Reviewing current research related to variables that influence cloud adoption, three research gaps emerged. Firstly, current research was delineated to the Netherlands and therefore failed to capture geographically specific variables, such as legal or cultural characteristics. Secondly, authors that analysed the decision-making process of adopting cloud technology neglected any interrelations between different variables. Thirdly, existing theories fell short in capturing the full scope of could computing adoption decisions, being either too generic or not specific enough.

To address the knowledge gaps and simultaneously fulfil the objective of this study, Interpretive Structural Modeling (ISM) and Fuzzy Matrice d'Impacts Croisés Multiplication Appliquée à un Classement (MICMAC) methods are used. ISM aims to simplify complex relationships between a system of variables by providing a graphical representation of the hierarchical structure of that system. Fuzzy MICMAC is used to assess the strength of the relationship between the variables. In total, 22 interviews with experts in the field were held as input for the analysis. The experts worked in the Dutch public sector and were familiar with the decision-making process related to cloud computing adoption.

In the first step of ISM, relevant current literature and official Dutch documents and reports were used to create a list of eight variables that would have a negative effect on the decision to adopt cloud computing within the Dutch public sector. These were classified as the 'barriers'. Additionally, a list of eight positive variables was created and classified as the 'drivers'. Then, the ISM Fuzzy MICMAC steps were followed for both lists.

Key findings for ISM can be described as 'how many' other variables are influenced by a certain variable, or by 'how many' other variables this certain variable influences (including indirect effects). For Fuzzy MICMAC, results can be described by using the terms driving power, i.e. how

'strong' does a variable influence other variables in the system, and dependence power, i.e. how 'strong' is a variable influenced by other variables.

For the barriers, *Regulations and government policy* was the variable that had the most influence on other variables within the barrier system. The barrier that influenced other variables the strongest however (i.e. had the highest driving power), was *Lack of knowledge and capabilities*. Both *Internal resistance to change* and *Negative business case* were influenced by the highest number of other variables and did not affect any new variables. The variables with the highest dependence power were *Internal resistance to change* and *Data security concerns*.

For the drivers, *Bigger knowledge market*, *Ease of use* and *Improved hard- and software* were the variables that had the most influence on other variables within the drivers' system. The driver with the highest driving power was *Improved hard- and software*. *Governmental strategy* was influenced by the highest number of other variables and did not affect any new variables. The variables with the highest dependence power were *Lower and flexible cost* and *Governmental strategy*.

The findings of this research have practical and theoretical implications. Practical, because they can support decisions about cloud within the Dutch public sector. Theoretical, since the findings suggest new variables, interrelations and theories related to public cloud computing. Furthermore, it uses ISM Fuzzy MICMAC, which is often used in the context of novel technologies, but never before for cloud computing adoption decisions.

Future research could address the limitations of this study, such as the exclusion of a feedback loop from the experts during the identification of the variables. Alternatively, research could use the Total Interpretive Structural Modelling (TISM) method to investigate the relationships further.

Preface and acknowledgements

This is it, the final piece I will write for this thesis. Interestingly, it will likely be the first piece that you as the reader will encounter. When I started with this thesis, I expected it to be stressful and a lot of work. In hindsight, it wás stressful and a lot of work, but it was also fun, engaging and never boring. Let's just say that it was a wonderful challenge.

A wonderful challenge I luckily did not have to tackle alone, and I therefore want to take a moment to thank the people who helped me during this journey.

Firstly, the incredible people that I met two years ago when I started the Management of Technology master's and can now very proudly call my friends. Julia, Stanley, Renzo, Fin, Felix, Masa, Saskia, Nikki, Thomas, Niklas and Ellen. You made my time during Management of Technology unforgettable and I cannot wait to see what you all will achieve in the future. You rock.

I would also like to extend my gratitude to all the members of my graduation committee. My chair and first supervisor, Prof. Dr. Ir. Nitesh Bharosa, for helping me shape my research and making sure I would keep my feet on the ground, even if my head was in the clouds. My second supervisor, Dr. Geerten van de Kaa, for asking critical questions that guarded me from crossing my own limits. My external supervisor Gina Plat, for providing excellent guidance and support when I needed it. And my advisor, Dr. Jacobien Oosterhoff, for helping me make sense of the chaos that was in my head for fuelling my enthusiasm for research in general.

Furthermore, I want to thank my colleagues at Deloitte, for their continued support and efforts to include me. Even though I was writing this thesis on my own, I still felt part of a team. Special thanks to Fons. The patience and understanding you showed while helping me with my programming endeavour was admirable, and your unwavering belief in my potential made me always want to strive for the best.

Moreover, I want to express my gratitude to all participants of this study for generously contributing their time and expertise. Thank you for all the fascinating conversations and the invaluable insights that ultimately shaped the findings of this research.

I want to thank my parents for their loving support and for allowing me to take care of my Thesis while they took care of me. Mom, thank you for constantly and always cheering me on and encouraging me to never give up. Dad, your constant feedback made my thesis what it is today and I am eternally grateful for all the time you put into reading it and commenting on it, even though the PDF format made commenting extremely difficult. But also the rest of my family, Timon, Laura, Paulien and Kristan, for their faith in my academic abilities.

Lastly I would like to thank Thijs, for always being my safe haven. I could not have done this without your love and support.

And thanks to you, the reader, for showing interest in my work. I hope you learn something from it, because I certainly did.

Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Definition	English translation (if applicable)
AC-ICT	Advies Comissie Informatie en Communicatie Technologie	Advisory Committee Information and Communication Technology
AP	Autoriteit Persoonsgegevens	Dutch Data Protection Authority
AWS	Amazon Web Services	
BIO	Baseline Informatieveiligheid Overheid	Baseline Infomationsecurity Government
BR	Barrier	
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	The Ministry of the Interior and Kingdom Relations
CAPEX	CAPital Expenditures	
CIP	Centrum Informatiebeveiliging en privacy bescherming	Centre for information security and privacy protection
COVID-19	Corona Virus Disease 2019	
CSC	Cloud Service Consumer	
CSP	Cloud Service Provider	
DDOS	Distributed Denial Of Service	
DigiD	Digitale Identiteit	Digital Identity
DOI	Diffusion Of Innovation	
DR	Driver	
e.g.	exempli gratia	for example
FDRM	Fuzzy Direct Reachability Matrix	
FRM	Final Reachability Matrix	
GCP	Google Cloud Platform	
GovTech	Combination of Government and Technology	
IaaS	Infrastructure as a Service	
ICT	Information and Communication Technology	
i.e.	id est	that is
ISM	Interpretive Structural Modelling	
IT	Information Technology	
MICMAC	Matrices' Impacts Cruises Multiplication Applique a un Classement	
NIST	National Institute of Standards and Technology	
OPEX	Operational Expenditures	
OS	Operating System	
PaaS	Platform as a Service	
PvEeW	Programma van Eisen en Wensen	Concept of demands and wishes

RADIO	Rijksacademie voor Digitalisering en Informatisering Overheid	National Academy for Digitisation and Informatisation Government
RM	Reachability Matrix	
ROI	Return On Investment	
SaaS	Software as a Service	
SSIM	Structural Self Interaction Matrix	
TAM	Technology Acceptance Model	
TISM	Total Interpretive Structural Modelling	
TOE	Technology Organisation Environment	
TU	Technische Universiteit	Technological University
USD	United States Dollar	

1 Introduction

This chapter will start with the background and context of the thesis, after which the problem that the thesis will address is introduced. After that, the demarcation of the multi-actor GovTech problem is presented to provide context and further understanding. Then, the research objective and questions will be presented. The chapter concludes with the outline of the research design.

1.1 Background

In 1961, Professor John McCarthy predicted that one day, computation might be organised as a public utility. Subscribers would have access to a very large system of resources but only pay for the computing power and services they needed (Daylami, 2015). It wasn't for another 45 years however, when McCarthy's prediction became reality and Amazon Web Services (AWS) first introduced 'public utility computing', now known as cloud computing, to the wider market in 2006. AWS, becoming the first 'Cloud Service Provider' (hereafter: CSP), created a platform where its Cloud Service Customers (hereafter: CSC) got pay-as-you-go access to virtual servers and data storage space (Marston et al., 2011).

Not long after AWS, Google introduced its own Google Cloud Platform (GCP) in 2008 (Marston et al., 2011), followed by Microsoft Azure in 2010 (Qian et al., 2009). At first, these CSPs mainly moved applications that ran on in-house computers or servers to servers of the CSP on a "virtual machine" (VM). These computers were like the computers that people had at home, but accessible through the internet and with all the hardware in one place, managed by the CSP. Later the possibilities evolved as the CSPs made it possible for multiple users to share the same hardware, lowering overall cost. This idea of hardware optimisation extended even further with the evolution into serverless cloud computing: no dedicated hardware; the hardware would only be used - and paid for - when it was actually needed.

The provision of hardware is managed automatically with set parameters. In addition to this, different deployment models were introduced, based on the structure of, and the access to, the cloud services: public cloud, Private cloud and Hybrid cloud. In all three cases, the dedicated hardware is managed by the CSP. However, in the Private cloud deployment model, only a single organisation can use the particular dedicated hardware, whereas in the public cloud model, multiple customers can use the same hardware. The Hybrid cloud model uses a combination of public and Private cloud models. For completeness: On-premises means that the dedicated hardware is used, as well as managed, by the organisation itself.

Businesses started to incorporate cloud in their IT landscape, either seeing the possible advantages it could bring, like the disposal of their in-house data centres and thus saving costs, or to be ahead of the competition. This cloud adoption trend made a steep rise over the years. Gartner estimates a total end-user spend-age of 591.8 billion USD for public cloud services in 2023 (Gartner,

2022).

As with a lot of innovations, (private) businesses were relatively quick to adopt this technology in comparison with the public sector (Aziz et al., 2013). A distinction that could be related to the fact that public bodies are bound by legal frameworks that differ significantly from private ones, and have responsibilities in the public interest to ensure both availability and security of data. As a consequence, when public bodies consider the cloud as an option, a possible first step could be to create a uniform protocol for the legal classification and treatment of public sector data (Gleeson & Walden, 2016).

In the Netherlands, such a uniform protocol was published in the summer of 2022. The 'government-wide cloud policy' (Rijksbreed Cloudbeleid 2022) stated that under strict conditions, organisations within the Dutch public sector[1] would be able to use commercial public cloud services (Rijksoverheid, 2022). At that point, cloud services were already in use within the public sector but mostly in the form of private cloud structures. The reason that was given for the approval of (commercial) public cloud technology was the significant decrease in risks related to its use. The risks were mainly related to security, which had improved rapidly during the COVID-19 pandemic.

The change in Dutch policy enabled organisations in the Dutch public sector to start investigating their options for digital solutions that incorporated commercial public cloud technology. However, approximately a year after the policy has gone into effect, there is still a lot of hesitation about migrating to public cloud. The government, as well as the organisations that consider migration, recognise the potential that public cloud has, such as access to better hard and software (Ha, 2022), better security and availability (Hsu et al., 2014), and scalability and flexibility (Hsu et al., 2014). All these factors could also be achieved in a non-cloud setting, but often against substantially higher costs (Ha, 2022).

Still, numerous challenges that prevent effective adoption need to be faced. These challenges might be tied to agreements made between the CSC and CSP, such as how to ensure security and control of data (Jones et al., 2019) King and Raja, 2012, but also to a lack of compatibility between the current (IT) environment and a new cloud computing environment (Hujran et al., 2019). A strong legacy dependence, for example, will severely influence the choice to migrate to the public cloud (Nanos et al., 2019). In addition to this, human aspects such as a lack of knowledge and capabilities (Ali et al., 2016), as well as internal resistance, can form a possible barrier to adoption (Hsu et al., 2014).

These factors have been identified in previous literature, but to what extent are these factors recognised in the decision-making process within the Dutch public sector? And how do they relate to each other? Although CSPs often provide tools to help answer these questions, their motivation originates from gaining a competitive advantage and is not based on scientific research. As of yet, current research has not addressed these questions, so this thesis will aim to address these gaps.

[1]This policy did not apply to the Dutch public sector as a whole, and demarcated certain conditions for which organisations this would be possible, based on e.g. sensitivity of the data that was processed in that organisation.

Understanding the factors that influence the decision to adopt public cloud computing within the Dutch public sector is crucial to optimise its use and to accurately assess advantages but also consider disadvantages. This is necessary to make informed and strategic choices. This thesis aims at providing that understanding, by defining a concrete list of factors with a negative effect - and a list of factors with a positive effect - on the decision to adopt cloud computing within the Dutch public sector. The analysis of these factors will be done using Interpretive Structural Modelling (ISM) and fuzzy MICMAC, recognising any interdependence.

1.2 Cloud adoption as a multi-actor problem

The adoption of cloud technology can be viewed as a multi-actor GovTech problem (Bharosa, 2022). A GovTech problem, since it involves private (CSP) companies that offer their services and interact with the public sector. A multi-actor problem, since it involves multiple actors, all with their own interests and perspectives. The most important actors involved are:

- Policymakers (government agencies) need to provide a legal framework for the use of cloud computing services and make sure that the other actors adhere to current regulations.
- The Cloud Service Customers (CSCs): Entities in the public sector need to ensure that cloud computing services meet the requirements related to performance, conformity (continuity and alignment with current digital infrastructure), and compliance.
- The Cloud Service Providers (CSPs) are responsible for providing reliable and secure services that are in line with the requirements of the CSCs.
- The citizens are the end-users of the cloud solutions. They benefit from a secure, stable digital solution that is easy to use and protects their data.

The fact that this problem covers multiple actors can add to the complexity of it. In this thesis, the problem is viewed from the CSCs: the adopter or migrator. Even though some of the variables that will be introduced later on in this thesis also affect the other actors, it is still important to note that the starting point will always be the view from the CSC's perspective.

1.3 Research objectives and research questions

The objective of this study will be to investigate the landscape of variables that influence the decision to adopt public cloud technology.
The main research question is:

What is the interrelationship between variables that influence the decision to adopt public cloud computing within the Dutch public sector?

To help answer the research question, the following sub-questions will be answered:

1. What are the key variables that influence cloud computing adoption decisions?
2. What is the hierarchical structure between the variables?
3. What is the driving and dependence power of these variables? [2]

[2]The driving power means to what extent do variables drive other variables? The dependence power translates to the extent the which variables are driven by (i.e. dependent on) other variables.

1.4 Research design

In figure1.1, a schematic representation of the research design is presented. The research questions will be answered in the sections that they are connected to.

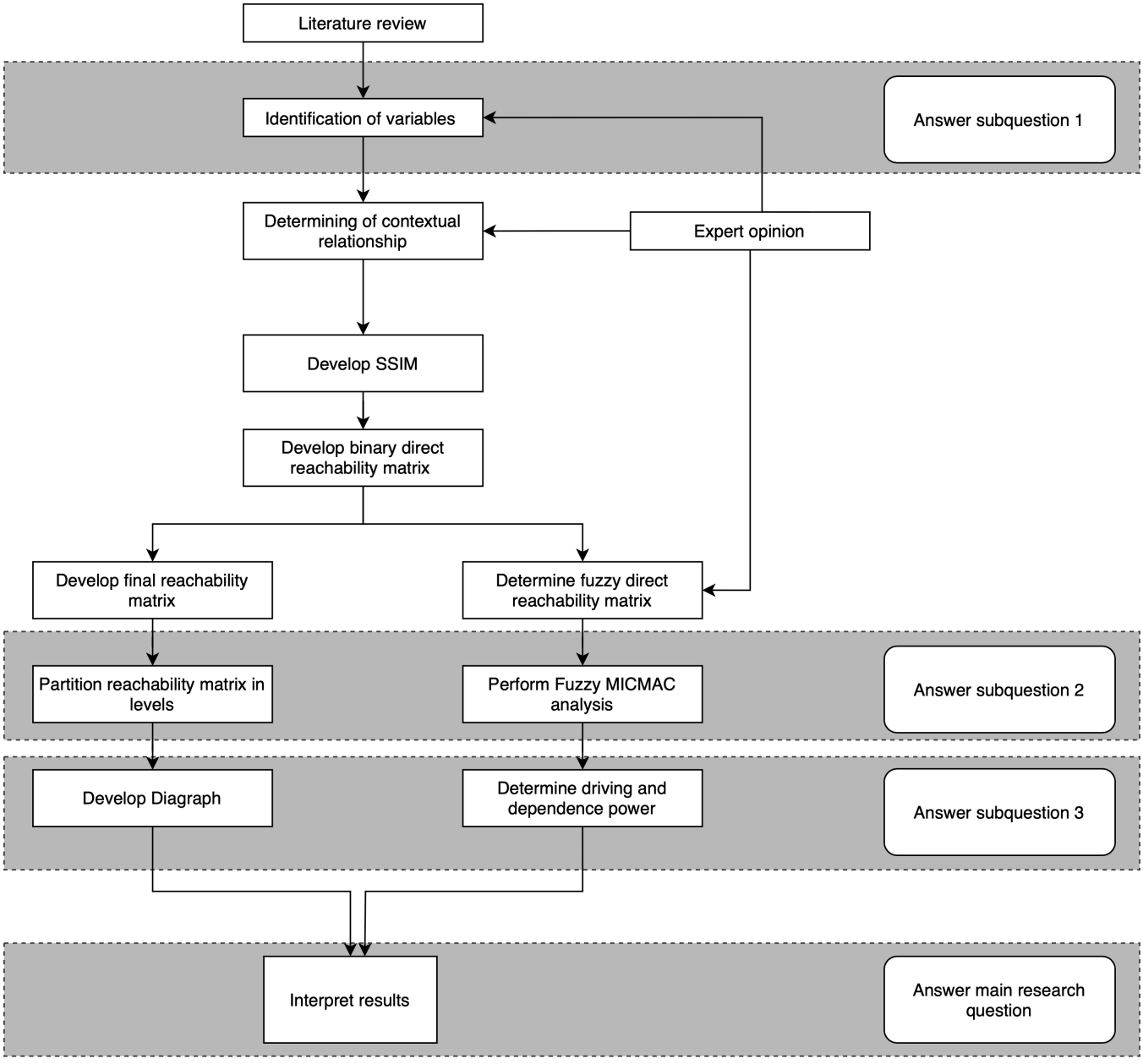

FIGURE 1.1: Research design

2 Literature review

2.1 Introduction and literature gaps

In preparation for this master's thesis, a literature review was performed that aimed at evaluating the state-of-the-art challenges related to cloud computing technology and the government. This literature review formed the foundation of this thesis and is presented in Appendix A.

Two research gaps that emerged from this literature review were:

- The lack of research that focused on the Dutch public sector specifically. Especially since public cloud adoption is influenced by national regulations, it is important to place research in its geographical context.
- Authors that analysed the effect of variables that influence the decision-making of adopting cloud technology only focused on the variable's influence on the 'final' outcome, and not on the influence that variables had on each other (e.g. (Hsu et al., 2014). For an adequate analysis of the landscape of variables that decision-makers should consider, interrelationships between the variables should also be included.

To address these literature gaps, this thesis aims to provide an analysis of the variables that influence cloud computing adoption within the Dutch public sector as well as the interrelations between these variables.

The first step in this process is defining the variables that will be represented in the analysis. To obtain them, a second literature study is performed to extract relevant variables from the current literature. In addition to this, current Dutch policies and reports are reviewed to identify variables that influence the decision to adopt public cloud technology. The findings of this second literature review are presented in this section.

This chapter is structured as follows: First, the search description, selection-, inclusion-, and exclusion criteria are described. Then the cloud concepts and relevant Dutch documents are presented. After that, the method for aggregating the final variables is outlined and the chapter concludes with a description of each variable that is included in this study.

2.2 Search description and selection criteria

2.2.1 Keywords and selection criteria

At the start of the literature review, an initial skim was done to identify the current developments of cloud use within the Dutch government. This search included non-scientific sources, such as podcasts and (reactions to) policy documents of the Dutch government. The main goal was to

find out which topics were perceived to be relevant. It is important to note these non-scientific sources were not used in the initial development of the variables, except for policy reports that were used as a checklist to cross-reference the variables for their relevance in relation to the Dutch public sector.

Before the keywords and selection criteria are presented it must be noted, that the decision of the Dutch government to allow public cloud usage was motivated by the fact that the cloud computing technology, and especially the security of its usage, improved significantly during the COVID-19 pandemic (Rijksoverheid, 2022). To accurately evaluate variables that were (and still are) present after this decision was made, it could be argued that relevant research was performed after the pandemic since the public cloud computing technology was at that point mature enough to be admitted to the Dutch public sector.

However, it was not possible just to include after-pandemic performed research, because of its significant lack in quantity and quality (e.g. "cloud computing, public sector, drivers" had only 1 hit after 2019, and 6 hits before 2019). Since the biggest change was made in the security field, research related to government and cloud usage in this area which was executed before the pandemic started (i.e. march 2019) was reviewed with extra care.

To find relevant articles, Scopus was used as a search engine. In some cases, articles were not accessible through Scopus and then Google Scholar was used. The keywords that were used are described in table 2.1. In every search, keywords or synonyms were combined to find relevant articles related to variables that influence cloud computing adoption in the public sector.

Keywords	**Synonyms**
Cloud computing	Cloud, Public cloud
Variables	Drivers, Barriers, Challenges, Opportunities, Strengths, Weaknesses, Benefits, Risks
Public sector	Government, e-Government

TABLE 2.1: Keywords and synonyms

Optional keywords are described in table 2.2. These keywords were not always included since they severely limited the number of articles that were shown in Scopus. For example, an initial search with the keywords "cloud computing" "government" and "Netherlands", resulted in 5 hits. This lack of sources underlined the need for scientific research in this field. However, the Netherlands has a rather small geographic scope and since a lot of the jurisdictional challenges that the Dutch government faces with regard to cloud migration are imposed by the EU, the search was widened by changing "Netherlands" into "Europe" which resulted in 30 hits. However, after evaluation it was determined that only a few articles considered relevant variables, so a third search omitted the geographical term altogether. This was done to enable robust (holistic) inclusion of variables that would be distilled into Dutch public sector related at a later stage, for which the method is described in section 2.5.2. Nevertheless, it is important to acknowledge that the literature review also considered dead ends and initial approaches that changed over the course of the research.

Optional keywords
Adoption, adoption decision
Netherlands, Europe
Influence

TABLE 2.2: Optional keywords

Additional useful articles were found by following the references of the research that was presented in the first articles that Scopus showed (snowball effect). Alternatively, research that referenced the "initial articles" was also included in some cases, based on the information in the abstract.

Articles that were found during the search for barriers were also used for the drivers and vice versa.

2.2.2 Inclusion and exclusion criteria

Since the topic of cloud computing technology in the public sector is a rapidly changing field, multiple sources were excluded because of their 'older' publication date. Since the NIST defined the cloud computing model as we still use it today in 2011 (Mell & Grance, 2011), sources older than 2011 were either excluded or evaluated more thoroughly on relevancy. The number of citations and the Field-Weighted Citation Impact[1] were also considered when selecting sources.

Due to the lack of relevant sources related to the Dutch public sector, there was a limited need to apply specific exclusion criteria. Research that focused on variables related to cloud computing and the public sector, in any specific field (e.g. technical, operational or environmental) or at any stage (e.g. regulation, implementation, or planning) was included. Some of the research focused only on e-government services, but since e-government services are part of government services in general, no distinction was made for the evaluation used in this literature review. Furthermore, wider research related to cloud computing technology which was not specific to the public sector was included if it sufficiently covered variables that would not be exclusively relevant for the private sector.

Even though they might not be considered 'scientific' sources, policy papers, governmental documents and official reports that were made by the Dutch government are included because they provide the current leading guideline for the Dutch public sector when it comes to cloud computing, and are therefore crucial when assessing the variables that influence a decision about that topic. A schematic overview of all inclusion and exclusion criteria is proved in table 2.3.

After the selection process, 27 articles and 4 reports were chosen to be included in this literature review. In appendix B, the search terms, total number of hits in Scopus and the articles that were ultimately included are recorded, which was determined by following the inclusion and exclusion criteria.

[1]The Field-Weighted Citation impact shows how well cited this document is when compared to similar documents based on publication year, document type and disciplines associated with its source.

Criteria	Inclusion	Exclusion
Period	Sources after 2011, with a preference for sources after 2019	Sources before 2011
Sector	Public sector, government and cross-sector research	Specific private sector research
Technology	Cloud technology, general factors of innovation	Other emerging technologies in the public sector that are unrelated to cloud technology
Research type	Peer-reviewed articles, case studies, scientific journals, policy papers, governmental documents and official reports	Blogs, forums, podcasts
Publication tool	Scopus, Google scholar	Other search engines
Country	Preference for Europe and non-USA	USA, but in some cases these were still used
Language	English, Dutch	Other

TABLE 2.3: Inclusion and exclusion criteria

2.3 Cloud concepts

For the definition of cloud computing and its different concepts the definition of the National Institute of Standards and Technology (NIST) is used. This is in line with the Government-wide cloud policy (in Dutch: Rijksbreed cloudbeleid) (Rijksoverheid, 2022) which played a significant role in shaping this thesis. This definition is also used in much more research (Zwattendorfer et al., 2013).

Cloud service, or cloud computing, is defined by the National Institute of Standards and Technology (NIST) as 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." (Mell & Grance, 2011). This is different from the traditional on-premise model, where the computer resources are installed locally. There are five essential characteristics of the cloud model, as defined by the NIST:

- *On-demand self-service*. Configurable cloud computing resources can be provisioned for the consumer (CSC) without requiring any human intervention (or interaction).
- *Broad network access*. Cloud computing resources are available through standard networks on heterogeneous client platforms.
- *Resource pooling*. The computing resources provided are pooled and used by multiple consumers at the same time.
- *Rapid elasticity*. Cloud computing resources can be scaled up or down automatically, depending on the CSC's needs.

- *Measured service*. Cloud computing providers monitor, control, optimise and report the usage of resources automatically, providing transparency for users and providers.

.
Following these characteristics, the cloud computation model can be categorised into *service models* and *deployment models*. These models will be described below following the definition of the NIST (Mell & Grance, 2011).

The service models can be distinguished by three different types of management by either the provider or the consumer of the cloud computing resources. The service models are:

- *Software as a Service (SaaS).* In the software as a service model, applications are provided to the customer. All other computing resources, e.g. hardware and networking, are hosted by the cloud provider. An example of Saas is Microsoft Office 365.
- *Platform as a Service (PaaS).* In this model, part of the computing resources is managed by the consumer (e.g. consumer-created applications) and part by the cloud provider (including network, servers, operating systems and storage).
- *Infrastructure as a Service (IaaS).* In this model, the consumer can provision and manage the most computing resources, such as arbitrary operating systems. The cloud provider only manages the underlying cloud infrastructure.

On - premises	Infrastructure as a Service	Platform as a Service	Software as a Service
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

CSP manages: CSC manages:

FIGURE 2.1: Cloud service models

In addition to the service models, four different deployment models are identified. The deployment models make a distinction in the features, structure, and access management of the cloud services provided. Deployment models:

- *Private cloud.* In this deployment model, the cloud infrastructure is exclusively provisioned for and used by a single organisation. It grants a firm greater control over the infrastructure and computational resources. It can exist on or off-premise.
- *Community cloud.* The cloud infrastructure is provisioned and used by a community of consumers and exists on or off-premise.

- *Public cloud.* The cloud infrastructure is provisioned and used by the general public and can be owned and managed by an organisation or a third. It exists on the premise of the cloud provider.
- *Hybrid cloud.* This is a deployment model that combines two or more of the other deployment models. These models can be used together, where the use of compatible technologies and data portability are of importance.

2.4 Current developments in the Netherlands

A fundamental task of the government is to support and provide services for individual civilians and society as a whole. This includes the delivery and availability of these services. Nowadays, people have become accustomed to digitally available services, mainly provided by the private sector. Companies such as Google and Microsoft introduced new opportunities for (data-driven) digital technology to the market, allowing the population to grow accustomed to a certain standard of IT services. The technological revolution of the (digital) service industry resulted in increased expectations of digital services in general. Theories of the government as a data-driven enterprise (van Donge et al., 2020) or a 'cloud' of public services (Alonso et al., 2016) are being explored, outlining a futuristic government that is capable of meeting the high expectations of our digitised society, but there are lots of bumps in the road. Cloud computing technology could be one of the enabling technologies that will help the government, and the public sector in general, to adapt and transform digitally.

Evidence of this shift in the digital landscape in the Netherlands was provided on the 29th of August, 2022, when it was announced that governmental bodies would be able to use commercial public cloud services (Rijksoverheid, 2022). Cloud services were already in use within the public sector but mostly in the form of private cloud structures, whereas this new cloud policy was directed specifically at the use of public cloud technology. The reason for this governmental approval of the (commercial) public cloud was that, at that point in time, the technology was considered mature enough and the advantages outweighed the risks (Rijksoverheid, 2022). The risks were mainly related to security, which improved rapidly during the COVID-19 pandemic since March 2020. The most important restrictions upon the use of public cloud services were that a mandatory risk assessment had to be carried out and that no state secrets were being stored or handled. Furthermore, no services could be conducted in countries with an active cyber program against the Netherlands (Rijksoverheid, 2022). The Ministry of Defense was excluded from this policy for security reasons.

Even though this policy change might indicate a desire to embrace cloud migration, no concrete strategy has been communicated for the adoption of cloud technology within the government until now and concerns about the new cloud policy have also been raised(Wolfsen, 2022). The Dutch Data Protection Authority (AP), stated that the new government-wide cloud policy does not adequately recognize the privacy risks associated with cloud computing and lacks methods to mitigate these risks (Wolfsen, 2022). Academic experts sounded the alarm bell after the cloud policy was presented, stating that the dependence upon American (cloud) companies could leave the Dutch public sector vulnerable (van Dijk & Jacobs, 2022). This accumulated distrust in several aspects of cloud technology eventually led to a motion that stated that the Dutch government should reconsider its newly produced cloud policy, to include European cloud alternatives and

focus on more data security (Hartholt, 2022). As of yet, the motion to adjust policy has not yet been treated by the Dutch government so the government-wide cloud policy remains in effect.

Within the Dutch government, several components (documents, departments and institutions) play an important role in cloud computing adoption. In the next sections, three of these components are described to provide a context of the current digital landscape in the Netherlands. These three components are used as input for the final list of variables that influence cloud computing adoption decisions in the Dutch public sector. This is presented in 2.5.

2.4.1 GDI and MIDO

The Generic Digital Infrastructure (GDI) is the collection of services, standards, and agreements that are used by all public service providers for their digital solutions to citizens and businesses.

The GDI is subdivided into five sections that have their own 'programming tables': access, interaction, data exchange, infrastructure and architecture. These sections are then again divided into digital 'building blocks', which represent digital applications such as DigiD. To enable inter-administrative cooperation, the Multiple Year Plan (MIDO), and Multiple Year Vision were set up in 2022 to transform the GDI and provide support for both public service providers as well as private parties with a public task (MIDO-kader, 2022) (BZK, 14-01-2022).

The MIDO provides an overview of the current and future digital infrastructure and its components and addresses trends for the coming years. For example, the 'programming table' infrastructure is expected to have an increase in the use of cloud technology (BZK, 14-01-2022). Whether 'public' cloud technology is meant remains unclear. Only for some specific building blocks the MIDO states that a private governmental cloud ("Rijkscloud") is used. This is in contradiction with the Dutch cloud policy 2022, which stated that a governmental private cloud could not be established due to a lack of coherent demand (Rijksoverheid, 2022).

The GDI and MIDO reports were used to establish a general overview of the current Dutch digital infrastructure. This provided the context in which to place the variables that were found in other reports and in the literature.

2.4.2 BIO

In October 2021, the 'Centre for Information security and Privacy protection' (CIP) published a reference framework to aid government organisations in their adoption of the cloud (Tewarie & van der Veen, 2023). It is in line with the Baseline Information security of the Government (BIO) and based upon the political developments, the input of the Dutch intelligence service and internal exploratory research.

The reference framework, often just named BIO, is structured by demarcating 'objects' that are of importance to the CSC, which is the public organisation in this case. The objects are analysed from the policy, execution, and control domains. The cooperation between the CSC and the CSP starts on the demand side with a 'Concept of demands and wishes' (PvEeW). In every step the following needs to be considered: Is the application of the cloud service in accordance with the

accepted risks by the Dutch government?

The next step is taken by the CSP, which is to make a functional and technical design. The design needs to comply with business and law demands. Additionally, the services need to be:

- Measurable and predictable
- Compliant with current law and regulations, and compliant with business and security demands
- Secure and controlled

Reasons for the government, and by extension the public sector, to use public cloud technology are identified in the BIO as:

- Focus on core tasks.
- Increase in efficiency of business operations and a decrease in total costs.
- The ability to acquire new IT functionalities quickly and therefore be able to adapt services to citizens and businesses more quickly to (changing) needs.
- Guarantee of qualified personnel.
- Lowering the IT complexity in specific situations.
- Improving security and availability.
- A revised business strategy and specific security requirements for processes and data.

The global structure and context of the cloud services are defined within a policy, execution, and control domain. Since the BIO is the most specified document in regards to Dutch cloud adoption it was chosen to cross-reference the variables with its contents. A description of this can be found in the appendix C.

2.4.3 AC ICT

The third relevant input is the assessment framework from the Advisory Committee of Infrastructure, Communication and Technology (AC-ICT) (ICT-toetsing, 2021). Projects within the Dutch public sector with a value above 5 million euros need to be checked by the committee. The assessment framework used by the advisory committee consists of nine risk areas:

- Business case, benefits and finance.
- Client and project organisation.
- Risk control and project dependencies.
- Consistency work processes and ICT solutions.
- Control of the scope.
- Architecture, Functional feasibility and technical achievability.
- Realisation and planning.
- Procurement aspects.
- Acceptance, implementation and transfer.

All of these areas are placed within the cloud computing technology context to assess relevant variables.

2.5 Variables

2.5.1 Shortcomings in the literature

In the introduction of this chapter, two literature gaps are presented that will be addressed in this research. In this section, another gap is highlighted: the lack of a universal method, model or framework to identify variables that influence the decision to adopt public cloud within the Dutch public sector.

Technology models that are used in the literature, such as Diffusion of Innovation (DOI) or Technology Operational Environment (TOE) are too narrow to provide a complete view of the relevant variables in this case. Both of them are made for smaller, demarcated technology, such as a specific app on a phone. Cloud adoption in the public sector stands for a large technological shift. Hence, these models are insufficient. Within the Dutch public sector, the AC-ICT will assess ICT projects in nine different areas which are deemed crucial in determining the feasibility of a project. However, these areas are determined for ICT projects in general and not tailored to cloud computing in particular and are hence insufficient to completely determine barriers or drivers. The same holds for the GDI and MIDO, which are set up broadly and not cloud-specific.

The BIO is an assessment form which is tailored for the Netherlands and for cloud Technology. It does denote important objects but mainly aims at mitigating risks, is subjective to the interpretation of the user and does not identify a concrete list of (negative) variables, and hence also provides insufficient input.

The objective of this thesis is to help managers and decision-makers in their considerations to adopt a public cloud within the Dutch public sector. However, the models used in the existing literature and the generalised nature of other reports fall short of capturing the full scope of this problem. There is no 'one model' or guideline that includes all variables relevant to the decision within the defined context. Therefore we have chosen to extract the most important variables from all of these sources and validate them using expert interviews.

At this point, it must be noted that the terms 'barriers' and 'drivers' might wrongly suggest that we should strive for a 'yes' on the question: should the Dutch public sector migrate to the public cloud? However, this thesis aims at supporting a decision with both outcomes (yes and no). If the question was posed differently e.g. should the Dutch public sector *not* migrate to the public cloud, the drivers and barriers would be switched entirely. To that end, all variables (barriers ánd drivers) can be seen as incentives to answer the question about public cloud use with either a 'yes' or a 'no'. Since it was chosen to use the opportunistic 'should the Dutch public sector migrate to the public cloud?', the 'no' incentives are coined as barriers and the 'yes' incentives as drivers [2].

2.5.2 Aggregation method

After an extensive review of the literature, the identified variables were aggregated and a distilled list was created to provide an overview of the elements that were relevant according to the current literature. The process of refining the variables involved analysis of the literature and putting an

[2] And even then, these 'incentives' can not unilaterally be ascribed to either the 'yes' or 'no' category, as many variables have a complex influence on adoption decision which includes both positive and negative parts

emphasis on the frequency of their appearance. If variables were consistently present in multiple studies, they were prioritised and proposed for the final list. This process was repeated for current Dutch cloud policy documents and for company documents from consulting firm Deloitte, based on their experience working with public sector clients.

Similar variables were grouped together to ensure that the variables covered a wide area of aspects that influence the decision to adopt public cloud technology within the Dutch public sector while having limited overlap. This was done with the help of an expert in the field and resulted in a list of 8 barriers and 8 drivers. Examples of the former are "lack of trust" (Alenizi & Al-karawi, 2022), "losing digital sovereignty" (Tewarie & van der Veen, 2023) (Ali et al., 2016) and "insecurity about data ownership" (Jones et al., 2019), which were grouped together and formed into "fear of losing control". The description of "fear of losing control" still included all the other variables, but it is nevertheless important to underline that a trade-off between completeness and conciseness (or compactness) was made during this condensing step. Since all experts who participated in the study were asked to validate the identified variables and provide new input, any one of them could have been chosen to act as the expert who helped in the condensing step. Therefore, the decision was made to use convenience sampling, and contact the expert who would be the most available to provide information (Sekaran & Bougie, 2016). While employing this method may not necessarily result in the most experienced expert giving input [3], it enabled frequent discussions and swiftly gained insights, which were considered of higher importance at this stage.

The final barrier list was cross-referenced with the BIO (Tewarie & van der Veen, 2023) to check if the variables were adequately represented. Since the BIO was mainly aimed at mitigating barriers (or risks), it was difficult to cross-reference the drivers with the BIO well. The drivers' list was therefore cross-referenced with the findings within company documents of consultancy firm Deloitte, which were based on their experience working with public clients. A schematic representation of the aggregation process is shown in figure 2.2 and the cross-reference lists are provided in C.

In ISM MICMAC it is quite usual to approach all experts that are willing to participate in the research at this stage. The identified variables are presented and altered if they, according to the experts, do not represent the relevant variables in the specified context (Junior et al., 2021). Due to time restrictions, the decision was made to not include the altering step of this 'feedback loop', and to ask for the expert opinion on the variables themselves during the interview (except for the one expert's opinion that was provided during the condensing step of the aggregation method). This has as a drawback that the variables might be solely based on literature and not accurately represent reality, which can in turn make it difficult for the expert to define the contextual relationship from one variable to the other. For example, how can expert A say something about the influence of variable i on variable j if it does not recognise variable i as having an influence on cloud adoption in the first place? However, it severely increased the amount of time needed to gather data, since an extra loop would mean knowing that people would participate in advance which was not feasible within the time limit of this thesis. Furthermore, using only literature for the variables is a method that is already established in previous research.

Since using (only) literature does raise the question whether or not the variables accurately represent reality, it was still asked during the interview. In most cases, the experts recognised all

[3] In the case of this study, the expert had 5 years of experience

presented variables from their experience. When the expert felt that a certain variable was not as strongly present, it was chosen to still include it because that variable might have a very strong influence on other variables that were deemed important by the expert, making them indirectly important to the system of variables as a whole.

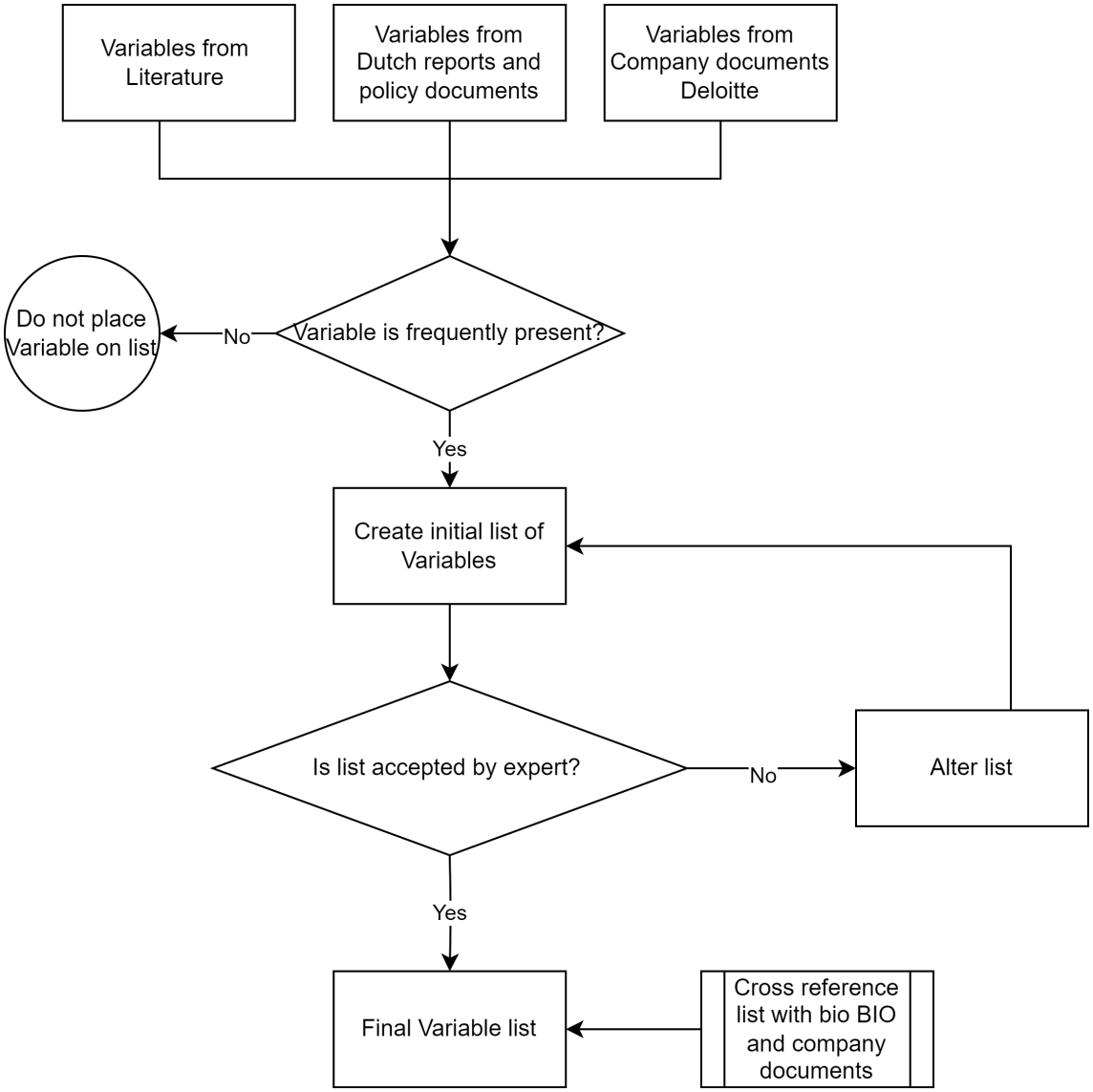

FIGURE 2.2: Schematic representation of variable aggregation

2.5.3 Barriers

In this section, the 8 barriers, i.e. the variables with a negative effect on the decision to adopt cloud computing within the Dutch public sector, are described. Long description:

- **Inadequate regulations and government policy**
  Regulations and government policy are often identified as a barrier in existing literature (Assaf et al., 2021) (Tewarie & van der Veen, 2023) (Abied et al., 2022a) (Hujran et al., 2019)

(Hsu et al., 2014). Existing rules and regulations are tailored to on-premise IT projects instead of public cloud IT projects. In addition to this, the Government-wide cloud policy only outlines cloud usage in a very general (vague) way, which could be interpreted differently based on subjective opinion (unlike e.g. the cloud-first strategy in the UK (Jones et al., 2019)). The absence, vagueness or (over)complexity of legal frameworks, regulations and government policy hinders cloud adoption in general, but especially in the public sector since it is in essence bound to governmental strategy and legal frameworks (Gleeson & Walden, 2016).

- **Data security concerns**
  Data security is defined as protecting data from unauthorised access, corruption, or theft (IBM, 2022). The cloud computing model characteristic of using shared resources and components could lead to increased system complexity and provide a larger 'attack area' where systems are vulnerable to hackers. Additionally, the internet delivery of public cloud services exposes government services to new network threats. All these concerns make it harder to guarantee data confidentiality and integrity within the public cloud (King & Raja, 2012) (Jones et al., 2019)(Ali et al., 2016) (Alonso et al., 2016).

- **Internal resistance to change**
  Unwillingness to adapt to new circumstances. public sector entities are known to be laggards when it comes to change (and new innovation), and this is no different in the case of cloud technology. Whether this is triggered by the high switching costs for training employees to use cloud services, the lack of need to gain a competitive advantage or the risk-averse mentality of its managers: there is an overall unwillingness to adapt to new circumstances which affect cloud adoption negatively (Hsu et al., 2014) Lee et al., 2012 (Nanos et al., 2019) (Zwattendorfer et al., 2013) (Halvorsen et al., 2005).

- **Legacy dependence**
  Governmental IT infrastructure often depends on soft- or hardware that has been superseded but is difficult to replace. These infrastructures are not compatible with cloud technology, increasing the costs of switching to the cloud (Mutkoski, 2015) (Aziz et al., 2013) (Nanos et al., 2019).

- **Lack of standards**
  This barrier is defined three-fold. There is a lack of standardisation on the CSC's side, e.g. different departments have different IT systems (also related to legacy dependency). There is a lack of standardisation on the CSP's side, which has a negative effect on the portability of the data that is handled in the cloud. Or there is a lack of institutional standards. The goal of this is that cloud services are usable on different IT platforms (thanks to standards) and that they can connect different platforms with each other (Interoperability). Data can be transferred to different CSPs without major modifications (Portability). (Zwattendorfer et al., 2013) (Tsohou et al., 2014) (Kotka et al., 2016) (Alenizi & Al-karawi, 2022).

- **Lack of knowledge and capabilities**
  The lack of IT-skilled personnel within the civil service, and the difficulty in obtaining enough IT-skilled personnel. Aside from the employees, the top management that is in

the end responsible for deciding to adopt cloud technology, is often lacking sufficient background knowledge in IT and cloud to make a well-balanced decision. Creating understanding and awareness can improve the accurate evaluation of all possibilities that cloud solutions could offer, which otherwise might be discarded based on a fear of undefined risks. In addition to this, a shift in knowledge is needed: from the operational/application administration that is needed in current on-premise environments to functional administration that is needed for cloud environments (Ali et al., 2016)(Alenizi & Al-karawi, 2022)(Aziz et al., 2013).

- **Fear of losing control**
  Placing public sector digital infrastructure and data at the disposal of a third party (the private sector-owned cloud) risks losing digital sovereignty. The shared responsibility model places most of the security controls of the CSC at the CSP. Even though the security agreement is checked on compliance and compared with an independent assurance report, it still leaves the CSC dependent on the CSP. Additionally, costs can increase if provider dependency becomes too high (vendor lock-in) (Alenizi & Al-karawi, 2022) (Jones et al., 2019) (Nanos et al., 2019) (King & Raja, 2012) (Ali et al., 2016).

- **Negative business case**
  The business case describes the use and need to start the (cloud migration) project, the costs and benefits and the boundary conditions. The business case can be interpreted financially, for example when the ROI is positive or not, but the aim of the business case is to support the choices, analyses and decisions that are made to start up the project. Alternatives are considered and a clear reason (for starting the project), problem statement and objectives are provided. Requirements are identified and analysed. The Advisory Committee ICT will test projects on this explicitly. If the business case is negative, it will most likely advise against starting the project at all (ICT-toetsing, 2021) (Ali et al., 2016)(Kuiper et al., 2015) (Mohammed et al., 2017).

The barriers were presented to experts in the field, in order to develop the contextual relationships between them. The exact method for this step will be described in chapter 3. The description that was used to describe the barriers is presented in table 2.4

Barrier	Description
Regulations and government policy	The absence of legal frameworks, as well as a uniform, governmental cloud protocol hinders cloud adoption
Data security concerns	Placing data and infrastructure in the public cloud can make it more vulnerable to attacks, due to network delivery and the increased amount of interfaces. Data integrity and confidentiality can therefore not always be guaranteed
Internal resistance to change	Unwillingness to adapt to new circumstances. Related to high switching costs (training), the lack of need to gain competitive advantage, and risk-averse management.
Legacy dependence	Existing IT infrastructure often depends on soft- or hardware that has been superseded but is difficult to replace. There is a lack of compatibility with cloud technology, making switching costs higher

Lack of standards	There is a lack of standards internally (legacy) and a lack of standards externally (strategic direction government) (no guarantee of data portability).
Lack of knowledge and capabilities	The lack of IT-skilled personnel within the governmental authorities, and the difficulty in obtaining enough IT-skilled personnel. Cloud possibilities could be better evaluated with more internal knowledge,
Losing control	Fear of losing digital sovereignty of data. Assurance and compliance issues, related to the shared responsibility model of CSP. Fear of a vendor lock-in which leaves the CSC to lose control to switch to a different CSP.
Negative business case	Insufficient substantiation for choice to use public cloud technology. Insufficient explanation about the 'need to migrate' often results in negative advice from the AC ICT.

TABLE 2.4: Compact description barriers

2.5.4 Drivers

In this section, the 8 drivers, i.e. the variables with a positive effect on the decision to adopt cloud computing within the Dutch public sector, are described.

- **Low and flexible cost**
  Lower costs to build and maintain hardware and resources (e.g. data centers), since the CSC can exploit the investments made by the CSP. An increase in the efficiency of business operations and fewer IT personnel is needed. Additionally, no on-premise licensing costs. Both CAPEX and OPEX are decreased when switching to the cloud, making this one of the biggest drivers according to literature. Other than lower costs, the pay-per-use pricing model allows for flexible costs (Pinheiro Junior et al., 2020) (Mell & Grance, 2011)(Qian et al., 2009) (Hsu et al., 2014) (Assaf et al., 2021) (Tewarie & van der Veen, 2023) (Marston et al., 2011) (Aziz et al., 2013) (Mutkoski, 2015) (Ha, 2022) (Mohammed & Ibrahim, 2015).

- **Governmental strategy**
  When the political debate is about the modernisation of the government, the government may choose to innovate by stimulating cloud use by adapting government cloud policy. The use of cloud technology makes public services themselves more agile to adapt to the changing digital needs of businesses and citizens. The push of a cloud-focused governmental strategy is a driver (Pinheiro Junior et al., 2020) (Tewarie & van der Veen, 2023) (Alenizi & Al-karawi, 2022).

- **Scalability, flexibility and agility**
  Cloud technology enables a lower development time, by configuring resources & scale up and down on demand. The latter also denotes the scalability (ability to scale your up/down on demand). This enables the CSC to focus on core tasks and provides a quicker response to changing requirements (agility)(Hsu et al., 2014) (Assaf et al., 2021) (Tewarie & van der Veen, 2023) (Halvorsen et al., 2005) (Mutkoski, 2015) (Mohammed & Ibrahim, 2015).

- **Larger knowledge market**
  Easier to find new personnel, since capabilities are widely recognised. This stands in contrast to private cloud on-premise solutions that are currently used in the public sector, which are dependent on highly specialised knowledge of that (unique) infrastructure. People retention will also grow since employees acquire external acknowledgement of the value of what they learn, ensuring them they are on a sustainable career path. Lastly, working with new technologies such as public cloud technology will attract more hires (Tewarie & van der Veen, 2023) (Ha, 2022).

- **Ease of use**
  Lowers the IT complexity in specific situations. Cloud resources are accessible via an internet connection and can be installed and upgraded easily in the console. Additionally, expert IT support is available to smooth out any problems, and no additional (complex) maintenance teams are needed (Hsu et al., 2014) (Assaf et al., 2021) (Tewarie & van der Veen, 2023) (Hsu et al., 2014) (Kotka et al., 2016).

- **Improving security and availability**
  The CSP has access to robust and advanced tech support, as well as soft- hardware in different availability zones, which protects the CSC against DDOS attacks and improves the

availability, and disaster recovery, of public services (Assaf et al., 2021) (Tewarie & van der Veen, 2023) (Hsu et al., 2014) (Mohammed et al., 2017) (Mohammed & Ibrahim, 2015).

- **Improved integration and interoperability**
  The cloud services are usable on different IT platforms and can connect different platforms, enabling integration and interoperability across departments and with third parties. Actions such as data sharing will therefore be more simplified (Hsu et al., 2014) (Elena & Johnson, 2015) (Ha, 2022).

- **More advanced soft- and hardware**
  A lot of the hard- and software used by the CSP is technologically more advanced and better tested than most of the current IT resources in the public sector (Marston et al., 2011) (Ha, 2022). In addition to this, advanced technologies that need a lot of computing power, such as AI can be realised easier (and cheaper) through the use of cloud technology than in an on-premise environment.

The drivers were presented to experts in the field, to develop the contextual relationships between them. The exact method for this step will be described in chapter 3. The description that was used to describe the barriers is presented in table 2.5

Driver	Description
Lower and flexible cost	Lower cost to build and maintain resources, less need for maintenance-focused IT personnel and less licensing costs.
Governmental strategy	A political agenda that pushes a cloud-focused strategy in order to innovate to answer to changing needs and demands of citizens and businesses
Scalability, flexibility and agility	Configuring and scaling of resources on demand and reduction of development time enables flexibility to focus on core tasks and agility to respond to changing requirements
Bigger knowledge market	Easier to find new personnel since capabilities are widely recognised (as opposed to private current solutions). Increase in employee retention, since an innovative workplace attracts and retains hires.
Ease of use	Cloud resources are easy to configure, and a lot of (complex) maintenance tasks are executed by the CSP.
Improving security and availability	Protection against large-scale cyber attacks (DDOS), faster disaster recovery and high availability
Improved integration and interoperability	Cloud services can connect to different IT platforms in a standardised way, improving integration, interoperability and data exchange across departments and with third parties.
Improved hard- and software	Access to technologies that are more robust and better tested.

TABLE 2.5: Compact description of drivers

3 Materials and methods

To determine the relationship between the different variables that were introduced during the literature review, ISM (Interpretive Structural Modelling) and fuzzy MICMAC (Matrices' Impacts Cruises Multiplication Applique a un Classement) are used. ISM is chosen to determine the interrelation between the variables holistically, while fuzzy MICMAC is added to gain more insight into the variables' driving and dependence power, which is determined by how strongly they influence, or are influenced by, other variables.

3.1 Overview

ISM was First introduced by Warfield in 1974 (Warfield, 1974) and aims to simplify complex relationships between variables in a system in order to provide hierarchical direction and clarity (Sage, 1977)(Warfield, 1974). The method consists of the following steps, which are explained in detail in the next sections:

- Variable identification
- Determining contextual relationships
- Developing Structural Self Interaction Matrix (SSIM)
- Developing Reachability matrix
- Level partitions and graph creation
- Analysing driving and dependence power using Fuzzy MICMAC

3.2 Variable identification

From existing literature and other relevant documents, variables related to the issue are identified. In this research, an extensive literature review is done to identify variables that influence public cloud adoption in the Dutch public sector. Additionally, the Baseline Information security Government (BIO) and the risk areas that are identified by the AC-ICT are included. The variables are categorised into drivers, which positively affect the decision to adopt cloud technology, and barriers, which negatively affect the decision to adopt cloud technology [1]. Since limited research is done in the field of cloud adoption in the Dutch public sector, the decision was made to include both the drivers and barriers in this research. To make the defining of the interrelationships between the variables easier, the drivers and barriers will be treated separately. This means that the

[1] As mentioned in 2.5, most variables are not unilaterally positive or negative, but the terminology is chosen to provide clarity and simplicity

subsequent steps are executed twice; one time for the barriers, and one time for the drivers.

3.3 Determining contextual relationships

Using experts' opinions, the contextual relationship between any two barriers (i and j), and any two drivers, is determined. To gather these opinions, several methods are described in existing literature such as individual interviews (Junior et al., 2021) (Amrina & Oktora, 2020), questionnaires (Dubey & Ali, 2014), or group sessions where a consensus is reached (Attri et al., 2013) (Dubey & Singh, 2015).

The main advantage of group discussions is that the participants will share different perspectives that are initially not evident for all individuals. The cross-participant collaboration that is needed to reach a consensus could result in more inclusive results. The main weakness of this approach is that the result is often biased by the ability of individual participants to express their arguments by expertise, determination or power (Junior et al., 2021). It is therefore impossible to assure the correctness of the consensus of a group discussion (Schuman, 2002). Minimisation of the group discussion bias is the main advantage of choosing the individual interview approach. On the other hand, the answers of the participants are highly subjective to individual perception which is the main weakness of using individual interviews (Junior et al., 2021).

In this research, individual interviews were chosen because of the aim to reduce the bias created within groups. In addition to this, the complexity of arranging a group discussion of relevant experts and the limited time available during the master thesis made it less desirable to choose that option. By choosing individual interviews, the data collection could be scaled up or down, depending on the number of participants that were found.

3.3.1 Participant criteria and selection

The criteria for the selection of the participants for the interview were:

- Participant is working for/in the Dutch public sector and her or his work is related to cloud adoption.
- The participant is familiar with the decision-making process of cloud adoption.

Initially, the criteria were limited to participants who were working *in* the public sector and were not extended to participants who were working *for* the public sector. However, it is usual for projects in the public sector, especially IT projects, to be created in cooperation with external parties (MIDO-kader, 2022). Therefore, the criteria were broadened to participants who work *for* the public sector, hereby including e.g. consultants and freelancers [2].

Additionally, a minimum amount of working experience years, either with cloud technology or in the public sector (and preferably both), was desired because this would validate the expert's

[2]It could be noted that these external workforces are still on the payroll of the public sector organisation so they are technically also working *for* the public sector but for clarity, the reasoning for including them is provided.

knowledge about the topic. However, since the Dutch policy only changed in the summer of 2022, it would be difficult to find participants working with the public cloud in the public sector for 3+ years. Therefore, the decision was made to leave the criteria as they were and to ask the participating experts about their years of experience based on IT and decision-making-related work within the Dutch public sector or work related to cloud technology. The decision was made to exclude academics from the study since the research focuses on the decision-making process from the perspective of the CSC (as described in section 1.2).

Participants were initially approached through the professional network of Deloitte and LinkedIn. After the first round of participant selection, the response rate was very low (3 participants were found). Previous studies that used the ISM fuzzy MICMAC single-interview-method included 4 interviews (Junior et al., 2021) minimum, and it was consequently decided that the lower limit was set on 5 interviews. The choice was made to do 5 instead of 4 to limit contradictory results in the expert opinions.

A second round of participant selection was initiated because of the low response rate of 3. More participants responded after changing the technique and approaching possible participants directly by contacting ministries and public organisations via email. In total, 38 experts were approached, and 22 of them participated in the study.

Table 3.1 gives an overview of the participants. In addition to the years of experience and the technical function name, a distinction is made between Technical and managerial/advisory roles. Participants with technical roles are involved in the design and implementation phase for IT solutions. These include for example architects, engineers and consultants. Participants with advisory/managerial roles oversee IT projects, provide strategic guidance, and make decisions about IT initiatives from a broader perspective. These include for example project managers, IT advisors, and policy makers.

3.3.2 Empirical validation and pairwise relation

After presenting the variables to the experts, they were asked if they recognised them in the field or if they noticed certain elements that were missing. Then, the contextual relationship between the presented variables was established [3]. This was done by exploring the pairwise relation between any two barriers (i and j), and any two drivers. In the literature, four types of pairwise relations between variables are identified (Bolanos et al., 2005) (Warfield, 1994):

- Definitive (includes, partitions, is a member of)
- Comparative (greater than, smaller than, more important than)
- Influence (causes, affects, enhances, supports, confirms, is independent of)
- Temporal (precedes, follows, is disjoint in time)

In this research, the type 'influence' is chosen because of the aim to better understand the interrelationship between the variables and not their definitive, comparative or temporal relation. In addition to this, the last three describe a static relation which does not provide insight into causal

[3]The reason for not including the expert's feedback on the variables in this stage is explained in section 2.5.2

#	Function name	Years of experience	Type of role
1	IT risk consultant	3	Technical
2	Cloud engineer	3	Technical
3	IT risk consultant	4	Technical
4	Sr. Manager Digital Transformation & Cloud	4	Managerial/advisory
5	Risk cloud engineer	5	Technical
6	Project lead cyber risk	5	Managerial/advisory
7	Partner Risk	8	Managerial/advisory
8	Project manager/product owner	10	Technical
9	Cloud Risk Advisory Director	13	Managerial/advisory
10	IT advisory	13	Managerial/advisory
11	Architect	13	Technical
12	Product owner	15	Technical
13	Advisor ICT	15	Managerial/advisory
14	ICT Architect	15	Technical
15	Advisor information security and privacy	18	Managerial/advisory
16	Partner public sector	20	Managerial/advisory
17	Product manager	20	Technical
18	Architect Team Test & Architect	20	Technical
19	Director Privacy & digital regulations	23	Managerial/advisory
20	Head of infrastructure/ product owner	25	Managerial/advisory
21	Sr. manager cloud engineering	25	Technical
22	Architect	28	Technical

TABLE 3.1: Overview of participants

relations.

The contextual relationship is thus established by asking the expert if variable *i* "influences" variable *j*. A supplementary explanation was given by stating that if a change would occur in variable *i*, would this trigger a change in variable *j*?

The process of asking about the pairwise influence was first repeated for all 8 barriers, and then for all 8 drivers. Since it was quite complex to establish all the relationships, it took approximately 1 hour per category. To ensure accurate data that were not biased by the participant being fatigued or rushed, there was a preference to discuss the barriers and drivers at separate appointments.

3.4 Developing Structural Self Interaction Matrix (SSIM)

After the determination of the contextual relationships, the direction of the relationships is noted in the Structural Self Interaction Matrix according to the following rules:

- V = variable i will influence variable j;
- A = variable j will be influenced by variable i;
- X = variable i and j will influence each other; and

- O = variable i and j are unrelated.

3.5 Developing the Binary Direct Reachability Matrix

In this step, the SSIM was transformed to the initial binary direct reachability matrix (BDRM) by substituting V, A, X and O by either 0 or 1, according to the following rules:

- If the (i, j) entry in the SSIM is V, then the (i, j) entry in the reachability matrix becomes 1, and the (j, i) entry becomes 0.
- If the (i, j) entry in the SSIM is A, then the (i, j) entry in the reachability matrix becomes 0, and the (j, i) entry becomes 1.
- If the (i, j) entry in the SSIM is X, then the (i, j) entry in the reachability matrix becomes 1, and the (j, i) entry also becomes 1.
- If the (i, j) entry in the SSIM is O, then the (i, j) entry in the reachability matrix becomes 0, and the (j, i) entry also becomes 0.

The diagonal elements were set to zero.

3.5.1 Aggregation of results

In previous research, various methods have been explored to aggregate the data from the individual interviews.

- Research by (Amrina & Oktora, 2020) considered the SSIM matrix and followed two rules: Firstly, the symbol (V, A, X or O) with the highest frequency of occurrence was selected for the aggregated SSIM. Secondly, if the frequency of a given relation was equal for 2 or more symbols, priority was given in the following order: V, A, X and O.
- Research by (Junior et al., 2021) considered the BDRM and assumed a value of 1 if half (or more) of the individual BDRMs had a value of 1.

Because of its potential to minimise the omission of data, the second option was chosen for this research. This can be illustrated by examining the situation in which one expert states that variable *i* influences variable *j* (symbol V), and another one states that variable *i* and *j* influence each other (symbol X). Following the first method, this would be a V in the aggregated matrix and the data of the expert who stated X will be discarded. However, if we use the second method, the data of X will be included since the ones in the RM will be added to the total value, therefore also increasing the threshold that needs to be crossed in order to establish a relationship in the aggregated matrix.

The *final* reachability matrix was subsequently determined by adding all entries of the BDRMs together and establishing the threshold for when elements are set to 1 and when to 0. After that, the diagonal elements of the aggregated BDRM were set to 1 and indirect relations were analysed by incorporating transitivity effects: if *i* influences *j* and *j* influences *k*, then *i* influences *k*. Using this method, both the direct and indirect effects are included. The final reachability matrix (FRM) was the base for the level partitions and diagram.

3.6 Level partitions and diagram

From the final reachability matrix, the reachability set and antecedent sets were derived. The reachability set consisted of variable i and all the variables that variable i would influence. The antecedent set also consisted of variable i but then included the variables that themselves influenced variable i. These reachability and antecedent sets were determined and based on their intersection, a distinction was made between different levels.

The levels were generated in the following manner: first, the reachability, antecedent and intersection sets for all the variables were established. Then, the variables for which the reachability and antecedent sets were the same will occupy the top level. The top level is occupied by the variables that have no variables 'above' them that they were influenced by. These top-level variables were then removed from all other reachability, antecedent and intersection sets and the process was repeated until all variables had an assigned level.

For example, say BR5 has a reachability set (3, 5, 6, 8), meaning it influences barriers 3, 6, and 8[4], and antecedent set (1, 3, 5, 6, 8), which means that barrier 1, 3, 6 and 8 influence BR5. It can now be concluded that BR5 only influences variables that it is itself influenced by, and does not reach any new variables. BR5 is now placed on the lowest level and 5 is removed from all other reachability and antecedents sets. Now, the intersection of the remaining variables is analysed and variables for which the intersection set is equal to the reachability set were placed on level 2 and removed from all the remaining sets. The process is continued until the final variable is assigned.

The diagram is created by placing the variables that were on the same level next to each other horizontally and adding arrows between them to show the relational direction.

After the graphs were constructed their face validity was tested by an expert in the field. This was done by asking the expert if she or he agreed with the connections that were present between the levels.

3.7 Fuzzy MICMAC

A limitation of the ISM method is that it only considers whether or not there is a relation, but it does not consider the *strength* of the relation.

3.7.1 Driving and dependence power

For ISM, relations were denoted by either a 1 if there is a relation, or by 0 if there is not. Fuzzy MICMAC is used to overcome this limitation, by enriching the relations with an additional degree of 'strength' that is denoted by a number in the interval [0, 1] (Bashir et al., 2022) (Khan & Haleem, 2012). The data for this degree of strength were obtained during the expert interviews that were held to establish the contextual relationship. In addition to the direction of the relationship, the opinion on the relationship's strength was considered according to table 3.2. Note that value 0 was automatically filled in if the expert stated that the variables had no influence on each other.

[4]Both the reachability and the antecedent sets also consist of the variable itself (Junior et al., 2021)

This method ensures that the importance of a variable is measured less by its direct relationships and more by many indirect relationships. These indirect relationships influence the whole system of variables through many reaction chains and feedback loops (Saxena et al., 1992).

Category	No relation	Very weak	Weak	Strong	Very strong
Value	0	0.25	0.5	0.75	1

TABLE 3.2: Linguistic and numerical values for strength relationship

The 'strength' value per relation was calculated and superimposed to the aggregated BDRM, which resulted in the Fuzzy Direct Reachability Matrix (FDRM). Two ways of aggregating these results are used in previous research which incorporated fuzzy MICMAC: the strength of the relationship was either determined by the strength with the highest frequency (Kamble et al., 2018) (Smania et al., 2022) or only one fuzzy matrix was provided that was created in consensus between the experts by approaching them a second time after the creation of the BDRM to provide their opinion (Khan & Haleem, 2012)(Junior et al., 2021) (Pfohl et al., 2011) if an explanation was provided at all (Dubey & Ali, 2014)(Deshmukh & Mohan, 2017). Due to time constraints, it was decided to minimise the number of contacts with the experts and the first method was chosen to determine strength was chosen as the fuzzy relationship. Moreover, the percentage of experts that stated a relation was already incorporated in the ISM section, by using the threshold of 70%. We could therefore state that only relations with a probability 'strength' higher than 70% were considered (Sushil, 2012). Thus, a relationship was included if more than 15 experts recognised it in the field, and the strength of that relationship was determined by the strength that was identified the *most often* by *all* experts.

In order to determine the strength of the indirect relation from variable i to j, three types of compositions are possible (Zimmermann, 1996): max-min, max-product and max-average. In this research, the max-min option is chosen since the minimal strength of the indirect relationship between variable i and j is denoted by the maximum of all possible minimal impacts from i to j (Kandasamy et al., 2007).

Following the steps as described in (Khan & Haleem, 2012), adapted from (Kandasamy et al., 2007), the matrix is multiplied using the max-min method using the following function:

$$C = A, B = \max k[(\min(a_{ik}, b_{kj}))], A = [a_{ik}] and B = [b_{kj}] \tag{3.1}$$

Starting with the FDRM, the matrix is multiplied recursively (according to 3.1) until stabilisation of the driving and dependence power arise. The driving power of variable i is the result of the sum of the power of variables that influence variable i, i.e. the sum of all entries for row i. The depending power follows from the sum of variables that are influenced by variable i, i.e. the sum of all of the entries in column i (Dubey & Ali, 2014). If the hierarchy of driving power and dependence power remains the same in alternate stages of multiplication for all variables, the matrix is stable (Saxena et al., 1992). These calculations were executed in a Python script using the libraries pandas and numpy. The code will be made available to the reader upon request.

3.7.2 Cluster classification

After generating the Fuzzy MICMAC stabilised matrix, the variables are classified into four clusters which are visualised in a quadrant, based upon their driver-dependence power (Khan & Haleem, 2012) (Kamble et al., 2018):

- Autonomous Cluster: variables with weak dependence and driving power. The autonomous variables can be found in the lower left of the quadrant.
- Dependent Cluster: variables with weak driving and strong dependence power. The dependent variables can be found on the lower right of the quadrant.
- Linkage Cluster: variables with strong driving and strong dependence power. The linkage variables can be found on the upper right of the quadrant.
- Independent: variables with strong driving and weak dependent power. The independent variables can be found on the upper left side of the quadrant.

4 Results

During the interviews, the first step was to validate the variables by asking the experts if they recognised them in the field or if they noticed certain elements that were missing. In the second step, the interrelation of each of the elements was determined by asking for each variable *i* if it influenced variable *j* or vice versa. In the third step, the strength of the influence was determined by asking the experts how strongly variable *i* influenced variable *j*.

4.1 Variables

In the first step of the interview, the variables that are described in tables 4.1 and 4.2 were presented and the expert was asked if he or she agreed with them. In addition to this, the expert was asked to identify any extra variables that were deemed important but not represented (enough) in the tables.

Code	**Barrier**
BR1	Inadequate regulations and government policy
BR2	Data security concerns
BR3	Internal resistance to change
BR4	Legacy dependence
BR5	Lack of standards
BR6	Lack of knowledge and capabilities
BR7	Fear of losing control
BR8	Negative business case

TABLE 4.1: Coded barriers

During the interviews, the additional barrier *Lack of (supply by the) market* was proposed. This barrier relates to the fact that, within the current demand package of the Dutch public sector, so far there is no supplier available that can answer to these demands. For instance, there is no European cloud provider that can offer the same services as e.g. Microsoft Azure. A second barrier addressed the *Segmented structure of the public sector* where all organisations are separately responsible for their link in the chain. This compartmentalised nature of the public sector in general, could hinder adoption since it means that a lot of steps have to be carried out several times.

On the other hand, internal resistance was not always recognised as a barrier. On the contrary, it was stated by some experts that there was so little resistance and that employees were pushing for change so that was seen as a driver.

For the drivers, an additional driver that was noted was *Supplier strategy* which relates to the fact that current suppliers of IT services to the public sector are switching to the cloud. They are

Code	Driver
DR1	Lower and flexible costs
DR2	Governmental strategy
DR3	Scalability, flexibility and agility
DR4	Bigger knowledge market
DR5	Ease of use
DR6	Improving security and availability
DR7	Improved integration and interoperability
DR8	Improved hard- and software

TABLE 4.2: Coded drivers

thereby 'forcing' the (public) user organisation to either switch suppliers or migrate to the cloud.

Furthermore, a bigger knowledge market was not always recognised as being present as a driver, but also in general. Even though cloud providers provide training to enhance knowledge, experts stated that there was still a significant shortage of IT personnel which made it difficult to acknowledge a bigger knowledge market as a factor of influence. In addition to this, lower cost and increased interoperability were also not always recognised. Like with internal resistance, experts sometimes noticed a trend in the other direction: costs would end up higher and interoperability would get worse.

4.2 Determining contextual relationships and SSIM

In the next step, the contextual relation was determined by examining the direction of influence between each pair of variables. The results are shown in table D.1. As described in section 3.4, the following rules were followed to construct the SSIM from the expert's opinion:

- V = variable i will influence variable j;
- A = variable i will be influenced by variable j;
- X = variable i and j will influence each other; and
- O = variable i and j are unrelated.

In table 4.3, only the relationship (V, A, X or O) with the highest frequency is shown. The exact number of experts that observed this relationship is shown in table 4.4. An example of an interpretation of the results is that of the 22 experts, 11 experts found a relationship X between BR1 and BR2. This means that 11 people stated that inadequate regulations and government policy (e.g. complex or lack of regulations and policies) and data security concerns (e.g. bigger attack surface in the cloud, data integrity and confidentiality) influenced each other.

In the following sections, remarkable results are highlighted, such as the relations that were recognised by either the most or the least experts.

The relationships that were recognised by most experts:

- 18 out of 22 experts stated:

  - BR6 (V) BR7 = Lack of knowledge and capabilities influences losing control
  - BR4 (V) BR8 = Legacy dependence influences negative business case

- 17 out of 22 experts stated:
  - BR5 (V) BR7 = Lack of standards influences losing control
  - BR6 (V) BR8 = Lack of knowledge and capabilities influences the negative business case

The relationship on which the experts disagreed the most was BR3 A BR8:

- 8 out of 22 experts stated a relationship A, which means that the negative business case influences the internal resistance
- 4 out of 22 stated a relationship V which means that internal resistance influences the business case.
- 5 out of 22 stated a relationship X (they influence each other) or O (they are unrelated).

	BR1	**BR2**	**BR3**	**BR4**	**BR5**	**BR6**	**BR7**	**BR8**
BR1 Inadequate regulations and government policy		X	V	O	V	V	X	V
BR2 Data security concerns			X	A	A	A	X	V
BR3 Internal resistance to change				A	A	A	A	A
BR4 Legacy dependence					O	A	O	V
BR5 Lack of standards						X	V	V
BR6 Lack of knowledge and capabilities							V	V
BR7 Fear of losing control								V
BR8 Negative business case								

TABLE 4.3: Aggregated SSIM barriers

For the drivers, the relationship which was established by the highest number of experts is shown in table 4.5. The exact number of experts that stated any particular relationship is shown in table 4.6. The frequency of all possible relationships can be found in appendix D. The relationships that were recognised by most experts:

- 17 out of 22 experts stated:
  - DR1 (A) DR3 = Scalability, flexibility and agility influence lower and flexible costs
- 16 out of 22 experts stated:

	BR1	**BR2**	**BR3**	**BR4**	**BR5**	**BR6**	**BR7**	**BR8**
BR1 Inadequate regulations and government policy		11	10	11	12	9	9	12
BR2 Data security concerns			12	10	10	15	11	15
BR3 Internal resistance to change				14	13	13	15	8
BR4 Legacy dependence					9	10	10	18
BR5 Lack of standards						9	17	14
BR6 Lack of knowledge and capabilities							18	17
BR7 Fear of losing control								11
BR8 Negative business case								

TABLE 4.4: Number of experts that identified the SSIM relation for the barriers

  - DR1 (A) DR7 = Improved integration and interoperability influences lower and flexible costs

The relationship on which opinions were most divided was DR2 V/A DR4:

- 6 out of 22 experts stated a relationship V, which means that governmental strategy (political agenda) influences the bigger knowledge market, or a relationship A, which means that the bigger knowledge market influences the governmental strategy.
- 5 out of 22 stated a relationship X (they influence each other) or O (they are unrelated).

On average, 12.25 experts recognised the same relationship for the barriers and 10.89 for the drivers. Thus, on average more experts were in consensus about the relationships for the barriers than for the drivers.

4.3 Developing reachability matrix

In this step, the SSIM is transformed to the initial Binary Direct Reachability Matrix (BDRM) by substituting V, A, X and O by either 0 or 1, according to the following rules (see also 3.5):

- If the (i, j) entry in the SSIM is V, then the (i, j) entry in the reachability matrix becomes 1, and the (j, i) entry becomes 0.
- If the (i, j) entry in the SSIM is A, then the (i, j) entry in the reachability matrix becomes 0, and the (j, i) entry becomes 1.
- If the (i, j) entry in the SSIM is X, then the (i, j) entry in the reachability matrix becomes 1, and the (j, i) entry also becomes 1.

	DR1	**DR2**	**DR3**	**DR4**	**DR5**	**DR6**	**DR7**	**DR8**
DR1 Lower and flexible costs		V	A	A	A	A	A	A
DR2 Governmental strategy			X	V/A	A	X	A	A
DR3 Scalability, flexibility and agility				O	X	V	A	A
DR4 Bigger knowledge market					A	V	V	O
DR5 Ease of use						V	V	X
DR6 Improving security and availability							V	A
DR7 Improved integration and interoperability								A
DR8 Improved hard- and software								

TABLE 4.5: Aggregated SSIM drivers

	DR1	**DR2**	**DR3**	**DR4**	**DR5**	**DR6**	**DR7**	**DR8**
DR1 Lower and flexible costs		14	17	12	13	15	16	12
DR2 Governmental strategy			9	6	12	8	7	9
DR3 Scalability, flexibility and agility				8	9	8	9	12
DR4 Bigger knowledge market					9	13	12	11
DR5 Ease of use						14	12	8
DR6 Improving security and availability							8	12
DR7 Improved integration and interoperability								10
DR8 Improved hard- and software								

TABLE 4.6: Number of experts that identified the SSIM relation for the barriers

- If the (i, j) entry in the SSIM is O, then the (i, j) entry in the reachability matrix becomes 0, and the (j, i) entry also becomes 0.

In the previous section, only the relationship with the highest frequency per pair of variables is presented. However, the SSIMs are still developed for all data sets. For the creation of the BDRM, all 22 SSIMs are separately converted to individual BDRMs using the rules described above. In other words: all datasets are included in this section, and for each relation separately it is determined if a relation was recognised by more than 15 experts. If that was the case, the relation was

included in the total BDRM.

4.3.1 Barriers

The final, aggregated BDRM is constructed by adding the binary matrices of all BDRMs together and using a threshold of 15 to decide which entries will be set to 0 (relationship is excluded) and which entries will be set to 1 (relationship is included). The sum of the BDRM entries from the 22 participants is shown in table 4.7.

	BR1	**BR2**	**BR3**	**BR4**	**BR5**	**BR6**	**BR7**	**BR8**
BR1 Inadequate regulations and government policy	0	21	12	8	17	11	15	12
BR2 Data security concerns	12	0	19	7	10	6	13	15
BR3 Internal resistance to change	5	14	0	5	5	9	6	9
BR4 Legacy dependence	4	14	17	0	8	10	9	19
BR5 Lack of standards	6	16	16	7	0	12	19	15
BR6 Lack of knowledge and capabilities	6	20	21	15	15	0	22	20
BR7 Fear of losing control	15	18	20	4	2	4	0	13
BR8 Negative business case	2	1	13	2	3	3	4	0

TABLE 4.7: Total sum of BDRM entries from 22 participants for the barriers

The relationships that were recognised by most experts:

- all experts stated that BR6 influences BR7 = A lack of knowledge and capabilities influences fear of losing control
- 21 out of 22 experts stated:
  - BR1 influences BR2 = Inadequate regulations and government policy influence data security concerns
  - BR6 influences BR3 = A lack of knowledge influences internal resistance to change

The relationship which was recognised by the smallest number of participants was BR8 influences BR2 = A negative business case influences data security concerns. Only one expert stated that this relationship was present in this context.

The results in table 4.7 do not include the transitivity[1] principle yet, as this step requires a binary matrix which is formed by imposing a threshold on the summed entries. In this study the choice was made for a threshold of 70%; i.e. if 70% of the experts say the relationship holds, the relationship is included in the aggregated matrix. Concretely, if $(22/100x70 = 15.4)$ more than 15 experts have a value of 1 on place (i, j) in their individual BDRM, a value of 1 is assumed on place (i, j) in the aggregated BDRM. If 15 or fewer experts have a value of 1 at place (i, j), the aggregated BDRM has a value of 0 at place (i, j).

[1]transitivity between three elements exists when a relationship is derived from one indirect connection. For instance, if x is related to y, and y is related to z; then x and z have a transitive relationship (Junior et al., 2021).

	BR1	**BR2**	**BR3**	**BR4**	**BR5**	**BR6**	**BR7**	**BR8**
BR1 Inadequate regulations and government policy	0	1	0	0	1	0	0	0
BR2 Data security concerns	0	0	1	0	0	0	0	0
BR3 Internal resistance to change	0	0	0	0	0	0	0	0
BR4 Legacy dependence	0	0	1	0	0	0	0	1
BR5 Lack of standards	0	1	1	0	0	0	1	0
BR6 Lack of knowledge and capabilities	0	1	1	0	0	0	1	1
BR7 Fear of losing control	0	1	1	0	0	0	0	0
BR8 Negative business case	0	0	0	0	0	0	0	0

TABLE 4.8: The final binary direct reachability matrix using a threshold of 15

To investigate the influence of the height of the threshold, the results are also calculated for a threshold of 14 experts and a threshold of 16 experts. These results are presented in the appendix E.

In the final step, the diagonal elements are set to 1 and the transitivity principle is included to incorporate indirect relationships. The results of the final reachability matrix are shown in table 4.9. Transitive links are denoted with a star (*).

	BR1	**BR2**	**BR3**	**BR4**	**BR5**	**BR6**	**BR7**	**BR8**
BR1 Inadequate regulations and government policy	1	1	1*	0	1	0	1*	0
BR2 Data security concerns	0	1	1	0	0	0	0	0
BR3 Internal resistance to change	0	0	1	0	0	0	0	0
BR4 Legacy dependence	0	0	1	1	0	0	0	1
BR5 Lack of standards	0	1	1	0	1	0	1	0
BR6 Lack of knowledge and capabilities	0	1	1	0	0	1	1	1
BR7 Fear of losing control	0	1	1	0	0	0	1	0
BR8 Negative business case	0	0	0	0	0	0	0	1

TABLE 4.9: Final reachability matrix including transitive relationships for the barriers

4.3.2 Drivers

The same process is repeated for the drivers. The results for the sum of all BDRM entries are presented in table 4.10.

The final direct reachability matrix is again developed by setting all entries above the threshold to 1, and all entries below the threshold to 0. The result is shown in table 4.11, for a threshold of 15, and in the appendix E for a threshold of 14 and 16.

After including the transitive relations, the final reachability matrix is established and shown in table 4.12.

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8
DR1 Lower and flexible costs	0	16	4	3	4	3	2	4
DR2 Governmental strategy	2	0	13	11	5	13	11	7
DR3 Scalability, flexibility and agility	20	17	0	11	13	13	9	7
DR4 Bigger knowledge market	13	11	9	0	10	16	15	6
DR5 Ease of use	15	14	15	11	0	20	16	10
DR6 Improving security and availability	16	15	11	3	7	0	14	8
DR7 Improved integration and interoperability	16	12	13	6	9	12	0	6
DR8 Improved hard- and software	14	10	14	8	15	16	15	0

TABLE 4.10: Total sum of BDRM entries from 22 participants for the drivers

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8
DR1 Lower and flexible costs	0	1	0	0	0	0	0	0
DR2 Governmental strategy	0	0	0	0	0	0	0	0
DR3 Scalability, flexibility and agility	1	1	0	0	0	0	0	0
DR4 Bigger knowledge market	0	0	0	0	0	1	0	0
DR5 Ease of use	0	0	0	0	0	1	1	0
DR6 Improving security and availability	1	0	0	0	0	0	0	0
DR7 Improved integration and interoperability	1	0	0	0	0	0	0	0
DR8 Improved hard- and software	0	0	0	0	0	1	0	0

TABLE 4.11: The final binary direct reachability matrix using a threshold of 15 for the drivers

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8
DR1 Lower and flexible costs	1	1	0	0	0	0	0	0
DR2 Governmental strategy	0	1	0	0	0	0	0	0
DR3 Scalability, flexibility and agility	1	1	1	0	0	0	0	0
DR4 Bigger knowledge market	1*	1*	0	1	0	1	0	0
DR5 Ease of use	1*	1*	0	0	1	1	1	0
DR6 Improving security and availability	1	1*	0	0	0	1	0	0
DR7 Improved integration and interoperability	1	1*	0	0	0	0	1	0
DR8 Improved hard- and software	1*	1*	0	0	0	1	0	1

TABLE 4.12: Final reachability matrix including transitive relationships for the drivers

4.4 Level partition

The level that a specific variable occupies is based upon the intersection of the reachability set (= set of other variables that that variable reaches) and the antecedent set (= set of other variables that reach that specific variable). For the barriers, these sets are denoted in 4.13. If the intersection set is equal to the reachability set, it means that the variable in question will not reach any 'new' variables. In table 4.13, BR3 has reachability set (3), meaning it influences no other barriers [2], and antecedent set (1, 2, 3, 4, 5, 6, 7), which means that barrier 1, 2, 3, 4, 5, 6 and 7 influence BR3. Thus,

[2]Both the reachability and the antecedent sets also consist of the variable itself (Junior et al., 2021).

BR3 does not reach any new variables and is assigned to level 1. The same logic applies to BR8, which is assigned to the same level. Consequently, BR3 and BR8 are removed from all sets, and we repeat the process from the start. At the second iteration, for both BR2 and BR4 holds that the reachability set, with 8 and 3 removed, is equal to the intersection of the reachability set with the antecedent set. Thus, without BR3 and BR8 in the system, they do not reach any new variables and are assigned to level 2. The process is continued until the final variable, in this case BR1, is assigned.

Variable	Reachability set	Antecedent set	Intersection set	Level
BR1 Inadequate regulations and government policy	1, 2, 3, 5, 7	1	1	5
BR2 Data security concerns	2, 3	1, 2, 5, 6, 7	2	2
BR3 Internal resistance to change	3	1, 2, 3, 4, 5, 6, 7	3	1
BR4 Legacy dependence	3, 4, 8	4	4	2
BR5 Lack of standards	2, 3, 5, 7	1, 5	5	4
BR6 Lack of knowledge and capabilities	2, 3, 6, 7, 8	6	6	4
BR7 Fear of losing control	2, 3, 7	1, 5, 6, 7	7	3
BR8 Negative business case	8	4, 6, 8	8	1

TABLE 4.13: Summary of level partition of barriers

The same process is repeated for the drivers and is shown in table 4.14.

Variable	Reachability set	Antecedent set	Intersection set	Level
DR1 Lower and flexible costs	1, 2	1, 3, 4, 5, 6, 7, 8	1	2
DR2 Governmental strategy	2	1, 2, 3, 4, 5, 6, 7, 8	2	1
DR3 Scalability, flexibility and agility	1, 2, 3	3	3	3
DR4 Bigger knowledge market	1, 2, 4, 6	4	4	4
DR5 Ease of use	1, 2, 5, 6, 7	5	5	4
DR6 Improving security and availability	1, 2, 6	4, 5, 6, 8	6	3
DR7 Improved integration and interoperability	1, 2, 7	5, 7	7	3
DR8 Improved hard- and software	1,2,6,8	8	8	4

TABLE 4.14: Summary of level partition of drivers

4.5 Creating graphs

To create the final graph, the variables are structured according to the level partition from the previous step. After structuring the variables hierarchically, arrows are placed according to their directional relationship based on the binary direct relations (table E.1 and table 4.11). The results for the barriers are shown in figure 4.1, and the results for the drivers are shown in figure 4.2
The graphs which still include the transitive links are presented in the appendix F.

After the graphs were constructed they were validated by an expert in the field. The expert agreed with all the connections that were present in diagram 4.1. However, for the drivers 4.2, the expert stated that there should have been a connection between DR4 and DR3, so between Bigger knowledge market and Scalability flexibility and agility. In addition to this, the connection between DR4 and DR7, as well as the connection between DR5 and DR3 were missing. The expert agreed with all the other connections.

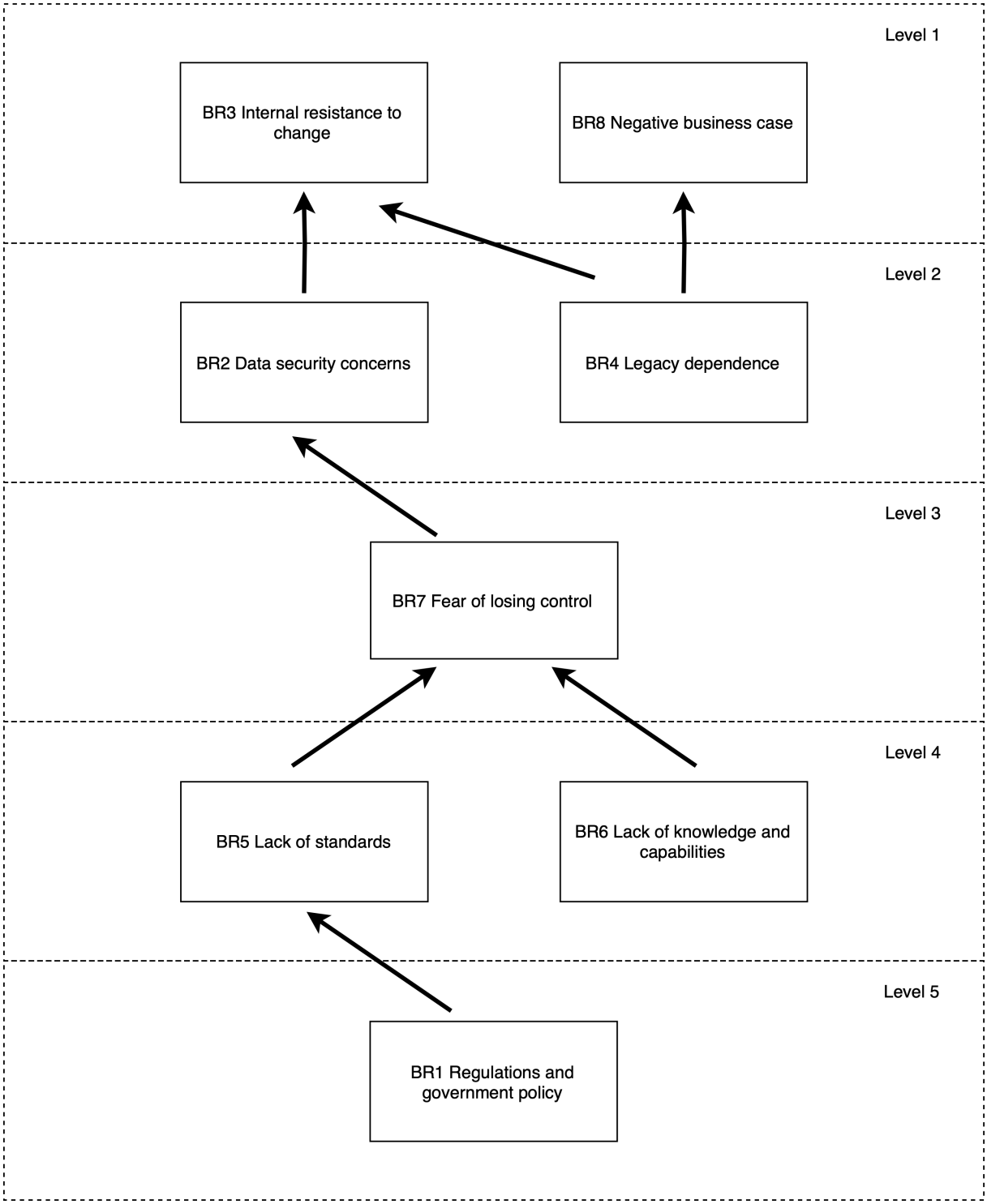

FIGURE 4.1: Final directed graph barriers

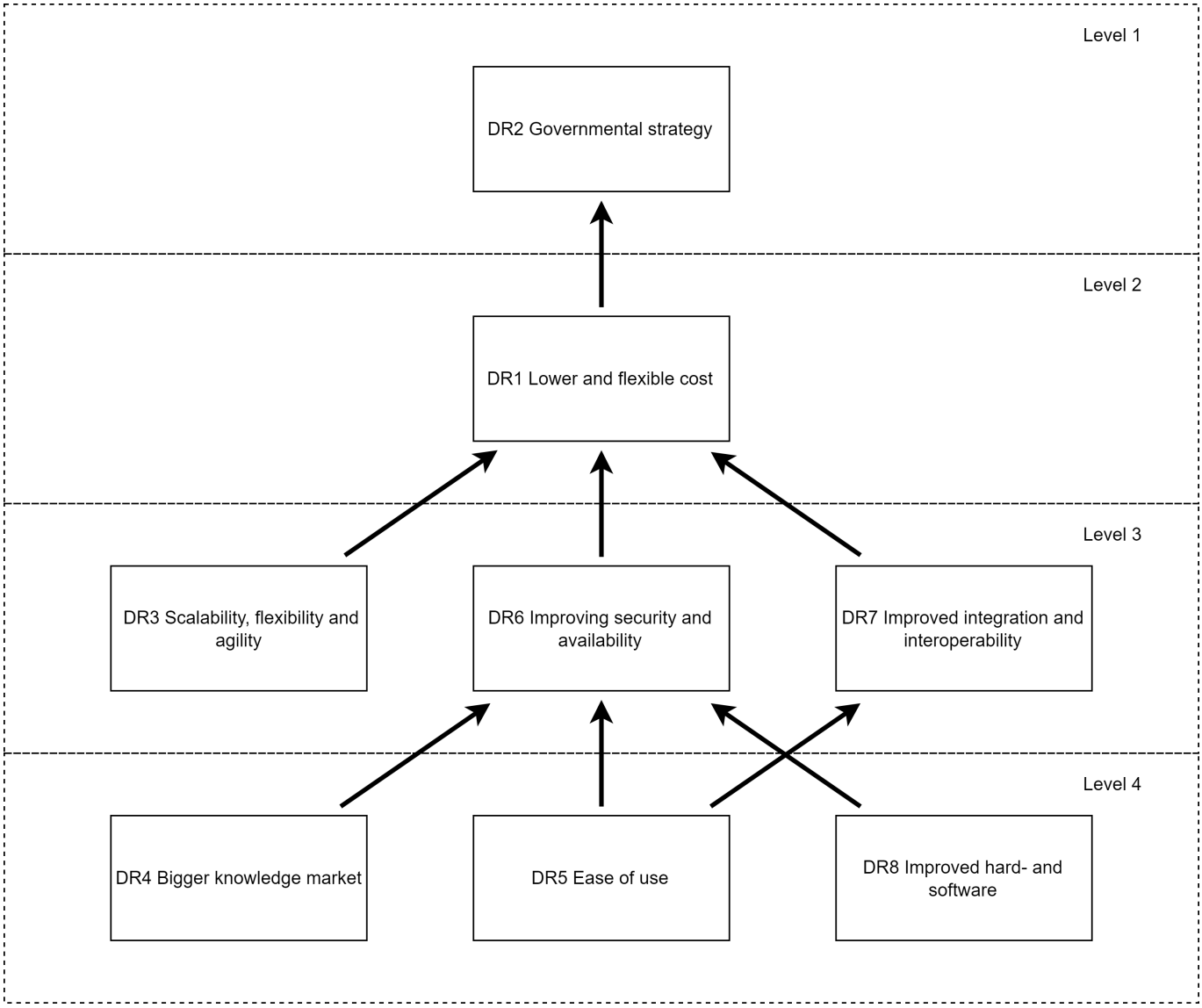

FIGURE 4.2: Final directed graph drivers

4.6 Fuzzy MICMAC

The fuzzy direct reachability matrix was determined individually by superimposing the numerical representation of the strength 3.2 to the BDRM 4.8 for all 22 participants. After this step, the aggregated fuzzy direct reachability matrix is constructed by taking the relationship with the highest frequency. Thus, it was determined by taking the strength factor that was recognised by the most experts of all individual fuzzy direct reachability matrices. The aggregated fuzzy matrix is shown in table 4.17. The diagonal is set to 1 as in Kamble et al., 2018 and (Khatwani et al., 2015).

	BR1	BR2	BR3	BR4	BR5	BR6	BR7	BR8
BR1 Inadequate regulations and government policy	1	0,75	0	0	0,75	0	0,75	0
BR2 Data security concerns	0	1	0,75	0	0	0	0	0
BR3 Internal resistance to change	0	0,75	1	0	0	0	0	0
BR4 Legacy dependence	0	0,75	0,75	1	0	0	0	0,75
BR5 Lack of standards	0	1	0,5	0	1	0	0,75	0,5
BR6 Lack of knowledge and capabilities	0	0,75	1	0	0,75	1	0,75	0,75
BR7 Fear of losing control	0,75	0,75	0,75	0	0	0	1	0
BR8 Negative business case	0	0	0	0	0	0	0	1

TABLE 4.15: Aggregated fuzzy direct reachability matrix barriers

In the next step, matrix multiplication is used as described by Kandasamy et al., 2007 using the formula:

$$C = A, B = \max k[(\min(a_{ik}, b_{kj}))], A = [a_{ik}] and B = [b_{kj}] \tag{4.1}$$

The matrix is recursively multiplied until it is stabilised and the levels of driving and dependence power no longer change.

After 3 iterations, stabilisation of the driving and dependence levels occurred. The matrix, the driving and dependence power, and levels are shown in table 4.16.

	BR1	BR2	BR3	BR4	BR5	BR6	BR7	BR8	Driving	Level
BR1 Inadequate regulations and government policy	1	0,75	0,75	0	0,75	0	0,75	0,5	4,5	3
BR2 Data security concerns	0	1	0,75	0	0	0	0	0	1,75	5
BR3 Internal resistance to change	0	0,75	1	0	0	0	0	0	1,75	5
BR4 Legacy dependence	0	0,75	0,75	1	0	0	0	0,75	3,25	4
BR5 Lack of standards	0,75	1	0,75	0	1	0	0,75	0,5	4,75	2
BR6 Lack of knowledge and capabilities	0,75	0,75	1	0	0,75	1	0,75	0,75	5,75	1
BR7 Fear of losing control	0,75	0,75	0,75	0	0,75	0	1	0,5	4,5	3
BR8 Negative business case	0	0	0	0	0	0	0	1	1	6
Dependence	3,25	5,75	5,75	1	3,25	1	3,25	4		
Level	3	1	1	4	3	4	3	2		

TABLE 4.16: Stabilized fuzzy matrix for the barriers

The results are visually analysed by creating a driving-dependence graph, which is shown in section 4.6.1. The same steps were repeated for the drivers, for which the results are presented in tables 4.17 and 4.18. In the case of the drivers, stabilisation also occurred after 3 iterations.

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8
DR1 Lower and flexible costs	1	0,5	0	0	0	0	0	0
DR2 Governmental strategy	0	1	0	0	0	0	0	0
DR3 Scalability, flexibility and agility	1	0,75	1	0	0	0	0	0
DR4 Bigger knowledge market	0	0	0	1	0	0,75	0,75	0
DR5 Ease of use	0,75	0,5	0,75	0	1	0,75	0,75	0
DR6 Improving security and availability	0,75	0,75	0	0	0	1	0	0
DR7 Improved integration and interoperability	0,75	0	0	0	0	0	1	0
DR8 Improved hard- and software	0	0	0	0	0,75	0,75	0,75	1

TABLE 4.17: Aggregated fuzzy direct reachability matrix drivers

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8	Driving	Level
DR1 Lower and flexible costs	1	0,5	0	0	0	0	0	0	1,5	7
DR2 Governmental strategy	0	1	0	0	0	0	0	0	1	8
DR3 Scalability, flexibility and agility	1	0,75	1	0	0	0	0	0	2,75	4
DR4 Bigger knowledge market	0,75	0,75	0	1	0	0,75	0,75	0	4	3
DR5 Ease of use	0,75	0,75	0,75	0	1	0,75	0,75	0	4,75	2
DR6 Improving security and availability	0,75	0,75	0	0	0	1	0	0	2,5	5
DR7 Improved integration and interoperability	0,75	0,5	0	0	0	0	1	0	2,25	6
DR8 Improved hard- and software	0,75	0,75	0,75	0	0,75	0,75	0,75	1	5,5	1
Dependence	5,75	5,75	2,5	1	1,75	3,25	3,25	1		
Level	1	1	3	5	4	2	2	5		

TABLE 4.18: Stabilized fuzzy matrix for the drivers

4.6.1 Cluster classification

After generating the Fuzzy MICMAC stabilised matrix, the factors are classified into four clusters based upon their driver-dependence power 4.3
4.3.
For the barriers, the results were:

- The Autonomous Cluster, i.e. the factors with weak dependence and driving power. This cluster is filled with variable BR4. Thus, within the system, the legacy dependence does (relatively speaking) not have much power to influence other variables and is also (relatively speaking) not influenced heavily by other variables.
- The Dependent Cluster, i.e. variables with weak driving and strong dependence power. This cluster is filled with variables BR2 and BR3. Thus, within the system, data security concerns and internal resistance to change have relatively little power to influence other variables, but other variables do have relatively high power to influence them.

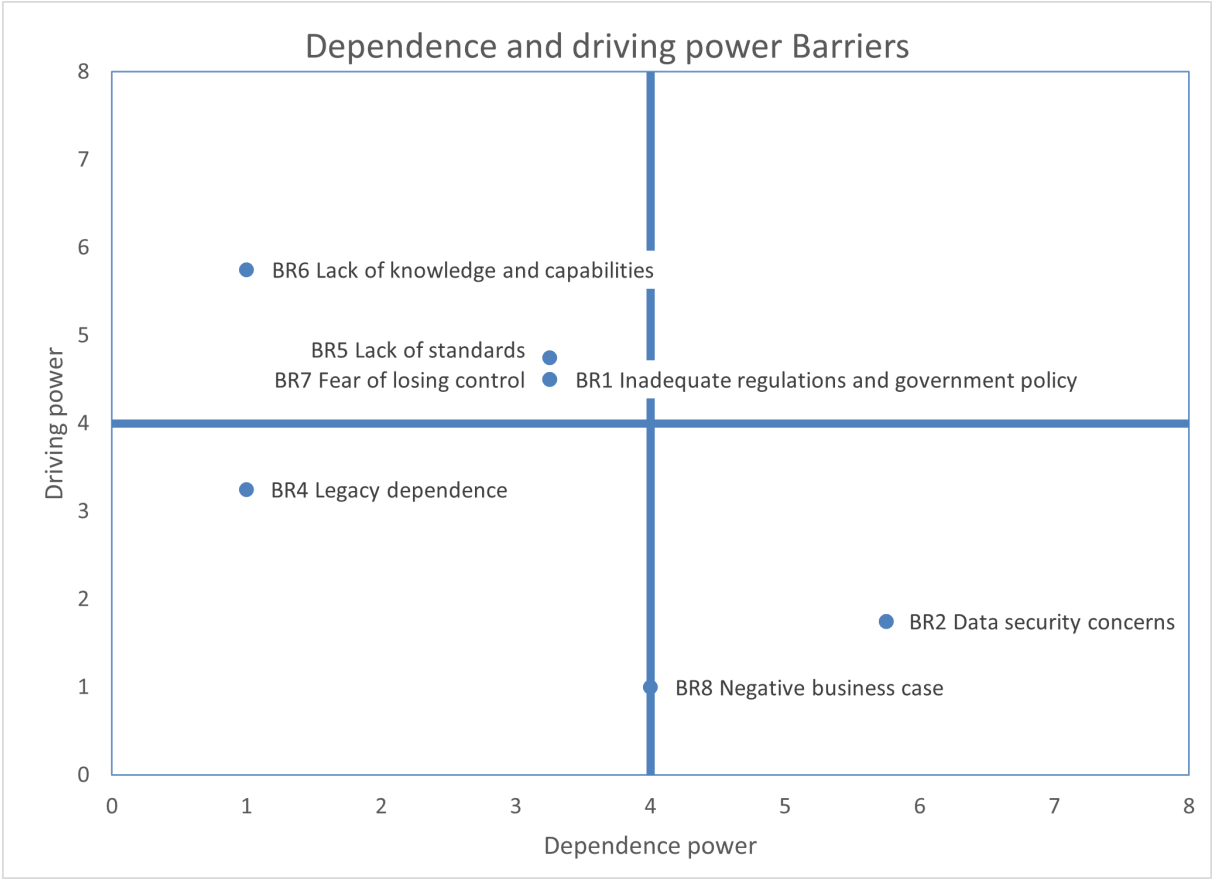

FIGURE 4.3: Driving and dependence power of barriers

- Linkage Cluster: variables with strong driving and strong dependence power. For the barriers system, there are no variables identified within this cluster.
- The Independent Cluster, i.e. variables with strong driving and weak dependent power is filled by BR1, BR5, BR6 and BR7. These variables are the least strongly influenced by other variables, but do have a strong power to drive others. BR6, i.e. the lack of knowledge and capabilities, has the strongest driving power in the system.
- BR8 lies exactly in the middle when it comes to the dependence power, and can therefore be counted to both the Autonomous and the Dependent Cluster. It has the lowest driving power of the system. To summarise: the business case has the least power to influence other variables and is influenced on an average level by other variables.

For the drivers, the results are presented in figure 4.4. The following cluster classification for the variables is identified:

- The Autonomous cluster, which contains variables DR3, DR6 and DR7. This means that within the system, scalability, flexibility and agility, improving security and availability and improved integration and interoperability have a relatively low driving power on the other variables in the system. At the same time, they are not dependent on other variables either since the dependence power is low.

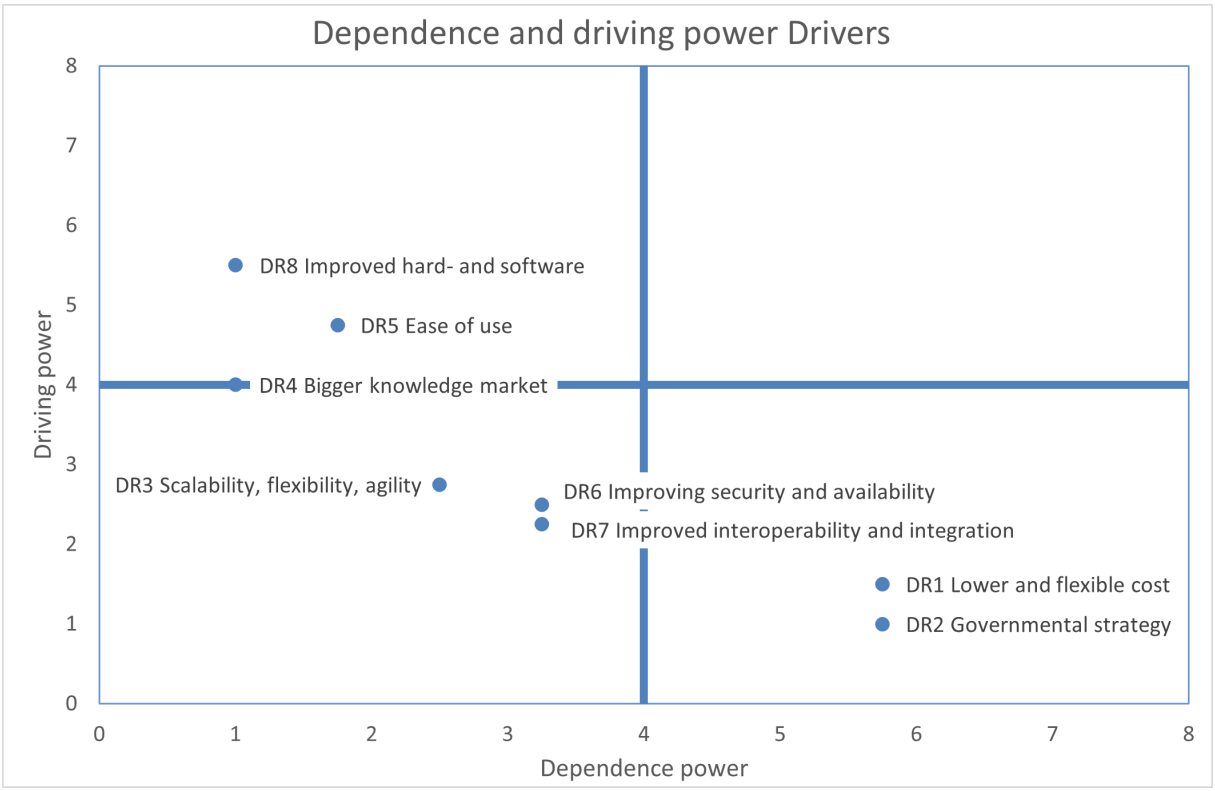

FIGURE 4.4: Driving and dependence power of drivers

- The Dependent Cluster contains DR1 and DR2, meaning that Low and flexible costs, as well as governmental strategy, have a low driving and a high dependency power. The governmental strategy has the lowest driving power in the system, meaning that the accumulated strength of its influence on other variables is the lowest.
- Linkage Cluster: variables with strong driving and strong dependence power. For the barriers system, there are no variables identified within this cluster.
- The Independent Cluster contains both DR8 and DR5. Improved hard- and software and ease of use strongly influence other variables, but are only weakly influenced by other variables. Improved hard- and software has the most driving power in the system.
- BR4, Bigger knowledge market, lies exactly on the boundary between the autonomous and independent quadrants, and can therefore be assigned to both clusters.

Since there are multiple variables that occupy the top level in the graph 4.2. The key variable is determined by the variable with the highest driving power, which is improved hard- and software.

For completeness, the aggregation is also performed by taking the average per entry (i,j) of all individual fuzzy matrices, after which the results were normalised. Even though averaging would include the most expert opinions, it would also 'flatten' them and presumably result in unrepresentative driving and dependence power. Furthermore, no existing literature was found that used the method of averaging the results for fuzzy MICMAC in this sense. These results can be found in appendix G.

5 Discussion

In the discussion section, possible explanations for the results are provided and the subquestions are answered. Furthermore, the limitations of the research as a whole are described and possible future research directions are outlined.

5.1 Discussion on results

In this section, the results are discussed. The three subquestions are answered throughout this section.

What are the key variables that influence cloud computing adoption decisions?

The key variables found in literature and Dutch reports and official documents, as far as the barriers are concerned: *Inadequate regulations and government policy, Data security concerns, Internal resistance to change, Legacy dependence, Lack of standards, Lack of knowledge and capabilities, Fear of losing control* and *Negative business case*. In addition to this and as described in section 4.1, *Lack of (supply by the) market* and *Segmented structure of the public sector* were proposed as barriers. *Internal resistance* was not always recognised.

An explanation for the last result could be that the participants of the study were all actively engaged in cloud-related environments and probably had an opportunistic perspective. In addition to this, participants needed to have knowledge about cloud technology and as seen in the results 4.1, a lack of knowledge influences internal resistance. The opposite could also be true: more knowledge leads to less resistance. Since the participants were highly knowledgeable, their perception of internal resistance could therefore be influenced.

For the drivers, the variables that were identified were: *Lower and flexible costs, Governmental strategy, Scalability, flexibility and agility, Bigger knowledge market, Ease of use, Improving security and availability, Improved integration and interoperability* and *Improved hard- and software*. In addition to this, *Supplier strategy* was proposed. *Lower and flexible costs, Bigger knowledge market and Improved integration and interoperability* were not always recognised.

An explanation for this last result could be that in most cases, the costs of using cloud services can exceed those of on-premise infrastructures. It was supposed however, that for cost comparisons, personnel or maintenance costs are not always included in the on-premise scenario, making it difficult to assess if the total costs are really higher.

The bigger knowledge market was often viewed as a very relevant variable which had not been noticed by many participants before. However, some of them noted that even though a nicer workplace and more training from cloud providers would mean more knowledge in the market,

there still was (and is) a large shortage of IT personnel.

According to some experts, interoperability and integration became more complex due to the incorporation of cloud services. This was not so much due to technical reasons, but more because of the broader (architecture) aspect since more parties were involved and issues related to how the cloud services would integrate with existing IT components increased.

In general, experts noted that the barriers were easier to recognise within the (Dutch) public sector specifically, whereas the drivers had a more universal background. This could originate from the fact that within the Dutch public sector, not many reports are available on driving variables. Presumably, CSPs offer their perspective on why cloud could be a viable option and the CSC feels the need to mitigate risks associated with the agreement with the CSP. It should however be noted that to make a well-balanced decision, it is important to address both drivers and risks from the CSC's perspective, independently from the CSP.

What is the hierarchical structure between the identified variables?

Following the ISM method, the level of variable *i* is determined by the intersection of the number of variables it (in)directly *influences* and the number of variables that it is (in)directly *influenced by.*

For the barriers, the variables were distributed over the different levels as shown in figures 4.1. The hierarchy starting from least influential/most influenced to most influential/least influenced can be summarised as follows:

1. BR3 *Internal resistance to change* and BR8 *Negative Business case* are occupying the lowest level in the system. They are relatively the least influential and the most influenced by other variables.

2. BR2 *Data security concerns* and BR4 *Legacy dependence* occupy the second level in the system.

3. BR7 *Fear of losing control* occupies the third level in the system.

4. BR5 *Lack of standards* and BR6 *Lack of knowledge and capabilities* occupy the fourth level in the system.

5. BR1 *Inadequate regulations and government policy* occupies the fifth and top-most level of the system. It is relatively the most influential and least influenced by other variables in the system.

Within the field, experts noted that a lot of the other barriers influence internal resistance directly, but that internal resistance mostly influenced others in a very implicit way. For example, having resistance to cloud adoption could slow the process of creating standards or the willingness to obtain new knowledge. However, the internal resistance would not be the 'main' influence in these processes and was therefore often not considered as a (very) influential variable.

The negative business case was often identified as having little to no influence on other variables, and was considered to be mostly influenced by the legacy dependence. Some experts also noted that a lack of standards makes it more difficult to construct a business in the first place since standards could be considered tools to develop a business case. In that sense, the lack of standards

did influence the business case, but not in a way that it induced a negative or positive outcome of the business case.

Regulations and government policy were often identified as a 'fixed' variable that could not be influenced by many others (except maybe a lack of knowledge). The regulations and government policy were set and therefore not changeable. Some experts noted that if the variable would also include (lower level) organisational rules and strategies, it might make it a more dynamic variable.

For the drivers, the following hierarchy was identified:

1. DR2 *Governmental strategy* is occupying the lowest level in the system. This is relatively the least influential and most influenced variable within the system.
2. DR1 *Lower and flexible costs* occupies the second level in the system.
3. DR3 *Scalability, flexibility and agility*, DR5 *Improving security and availability* and DR7 *Improved integration and interoperability* occupy the third level in the system.
4. D4 *Bigger knowledge market*, DR5 *Ease of use* and DR7 *Improved hard- and software* occupy the fourth and final level in the system.

Starting with level 1, it can be seen that governmental strategy is influenced directly by lower and flexible costs, which are in turn influenced by the other variables. A possible explanation for this is that all the technical aspects that can be realised with public cloud technology (e.g. improved security or improved integration) could in theory also be realised on-premise, but public cloud technology can offer these advantages at a lower price. The technical drivers, therefore, influence the lower and flexible costs, which in turn influence the governmental strategy.

It is also important to note at this point that the results of this section are based upon the *quantity* of other variables that were influenced. For example, a lot of experts stated that lower and flexible costs are not the most important driver to change governmental strategy, while graph 4.2 might suggest otherwise. Results related to which variables influenced others the strongest will be presented in the next section.

An interesting finding overall is that the two variables that 'come from' higher up in the government (DR2*Governmental strategy* and BR1*Inadequate regulations and governmental policy*) are either influenced the most or are the most influential. Incentives to say 'yes' to the public cloud within the public sector influence the governmental strategy, while the Regulations and governmental policy influence the incentives to say 'no' to the public cloud.

In general, it may be more accurate that incentives to say 'yes' to a new innovation could indeed alter a strategy, which can result in new rules and regulations to address incentives (when) to say 'no' to that innovation. This should however be a topic for further research. Additionally, a few experts noted that both of these variables were more 'enablers' than incentives, which could also explain their presence at either top or bottom levels.

What is the driving and dependence power of the identified variables?

To answer this subquestion, the definition of driving and dependence power is revisited: driving power means to what extent variables drive other variables and dependence power means to what extent variables are driven by (i.e. dependent on) other variables.

The driving and dependence power of all variables can be found in 4.4 and 4.4. In this section, the most important results will be discussed.

For the barriers, the variable which influenced other variables the strongest was BR6 *Lack of knowledge and capabilities*. This was entirely consistent with the opinion of most experts, who often denoted it as the most important variable in the system. The least driving power was assigned to the negative business case. Most experts did not link the business case to many other variables. A possible explanation for this is the fact that the business case in itself did not influence the variables, but more the next step of not starting a project: negative business case -> no cloud migration -> no knowledge development.

The barriers with the highest dependence power were *Data security concerns* and *internal resistance to change*. A possible explanation for this could be that data security concerns and internal resistance are often fueled by other incentives to say 'no' to public cloud computing. Aspects such as knowledge or standards can mitigate data security concerns as well as internal resistance, but a lack of them can have the opposite effect.

The barriers with the lowest dependence power were *Legacy dependence* and *Lack of knowledge*. Legacy dependence was usually noted by experts as a variable that existed due to 'fixed' technical reasons and was therefore not dependent on other variables. A possible explanation for the independence of the lack of knowledge could be that it is usually the result of a 'no' to the decision to adopt cloud technology. It is thus not influenced by the other variables, but more connected to the final outcome which is not included in the scope of this research.

The driver with the highest driving power was *Improved hard- and software*. During the interviews, it stood out that this driver was not linked to many other variables but íf it influenced another variable, it was usually a *strong* or *very strong* relation. This may have to do with the fact that improvement in hard- and software often has a very measurable effect (e.g. speed or capacity), making its influence 'strong'.

The driver with the lowest driving power was *Governmental strategy*. A possible explanation for this could be the fact that the governmental strategy in itself does not alter any other drivers, as it can be seen as a plan of action based on already existing variables. However, some experts noted that governmental strategy could influence the flexibility of organisations since it could help them in organising public cloud migration. It should be noted that governmental strategy was closely followed by low and flexible costs, meaning that the low and flexible costs also only influenced other variables in a very weak sense.

Drivers with the highest dependence power were *Lower and flexible costs* and *Governmental strategy* which were influenced the strongest by other variables. The reason for this could be that both variables are based on the other factors in the system. The fact that a public cloud solution can be realised with lower and more flexible costs is due to e.g. its technical scalability or its improved security. To achieve the same security standard, it is often more expensive to realise everything

on-premise instead of using public cloud which incorporates a lot of security measures in itself. As said in the previous paragraph, a governmental strategy is often based upon other variables in the system, making it highly dependent on them.

Drivers with the lowest dependence power were *Bigger knowledge market and Improved hard- and software*. The bigger knowledge market can be seen as an enabler for other drivers (especially if it is related to more IT personnel) but is rarely influenced by other (technical) variables within the specified system. For example, the fact that there is improved hard- and software does not necessarily influence the knowledge market. The improved hard- and software was often seen as a characteristic of the technology itself, which was not influenced by any external factors. It was however noted that a bigger knowledge market would in some cases lead to improved hard- and software.

5.2 Strengths and weaknesses

In this section, the strengths and weaknesses of the research are described, after which directions for future research are pointed out.

The strengths of the research were its new angle, the solidity of the study and its thoroughness.

The new angle of the research is evidenced by the fact that research on public cloud computing within the Dutch public sector was rarely done before, especially after the publication of the Cloud policy in 2022 (Rijksoverheid, 2022). In addition to this, the ISM Fuzzy MICMAC approach has never been combined with public cloud computing. This method lowered the complexity of interrelations, by providing a graphical representation of the hierarchy between the variables (Junior et al., 2021) (Sindhwani & Malhotra, 2016). Furthermore, by incorporating the strength of the relation, an extra dimension of analysis was added.

The solidity (or robustness) of the study is demonstrated by the fact that 22 experts were individually interviewed from many different departments and layers of the Dutch public sector. This is a relatively high number in comparison with other ISM Fuzzy MICMAC research, that included e.g. 5 participants (Junior et al., 2021).

The thoroughness of the study is substantiated by the extensive literature review that also included official Dutch documents to identify variables. The personal interview method also enhanced thoroughness, as that method granted the ability to clarify doubts and pick up on non-verbal clues (Sekaran & Bougie, 2016).

There are three categories of weaknesses that could be identified:

- In the data collection phase:
  - The expert's opinion was biased by the specific industrial setting where he or she was working in (Deshmukh & Mohan, 2017).
  - The interviewees were in some cases referred to by other participants, which could lead to biases.

  - Many interviewees who wanted to participate in the study, acknowledged the important role that (public) cloud technology could possibly take in the near future and felt positive about its use. It could therefore be the case that the sampling was biased towards cloud opportunistic experts. It could be argued that experts who did not acknowledge cloud technology as something that should be used by the government, also did not feel the need to participate in a study, and were therefore underrepresented.
  - The results of this study showed that a lack of knowledge is a large incentive to say 'no' to public cloud technology. However, the participant requirements stated that the interviewee must have knowledge about cloud technology and its decision-making process, which means that there could have been a bias within the sampling population.
  - In some cases, the interviewee did not agree with the identified variables, which resulted in complex discussions when establishing the influence of that variable on other variables.

- In the data analysis phase:
  - Only a limited number of variables are considered, and the problem or issue may consist of many more variables than the ones that have been identified in this study (Attri et al., 2013).
  - Variables that were included were only based on their frequency of appearance in literature and official documents. This may falsely result in the assumption that variables that have a high frequency are relevant. Even though input from experts was asked to explore the relevant variables in the field to overcome this limitation, new variables were still not included in the ISM fuzzy MICMAC analysis.
  - The results of ISM fuzzy MICMAC are not statistically validated (Attri et al., 2013).
  - Determining the strength of a relationship is highly subjective since it includes that participant's perception of 'strength', which could e.g. denote the possibility that something is related or the impact it makes if there is a relation.
  - To determine the strength of the relationship between variables, the interviewees were asked to assign one of five options. In reality, strength is not a discrete variable.
  - Because the final RM is based upon the inclusion threshold of 15 and is therefore subjective to the researcher's parameter choice.
  - ISM does not account for the interaction between variables on different levels. By removing transitive and bidirectional links, the reductionist graph can provide clarity. However, this does not always reflect practice. For instance, internal resistance could in practice influence regulatory changes, even though this is not reflected in the graphs.

- Overall:
  - Both methods do not arrange the variables in order of importance to the final 'public cloud migration' decision but rather rank them on how strong their influence is or how many other variables within the system they influence.
  - The relationships in the system are only denoted by direction or strength and are not further investigated, for instance answering the question of what the reasons are behind a claimed relationship.

5.3 Future research

For future research, the overall limitations of this study could be addressed. For example, letting the participants rank the individual importance of the identified variables on the final decision 'Should the Dutch public sector use public cloud technology'. This could address the criticism that the variables are now only analysed on their influence on each other, and not on their direct influence on the decision to adopt public cloud. Additionally, the simple question: 'Should public cloud technology be used within the Dutch public sector?' could be added to even out the sample of the experts to include positions that lean towards 'no', as well as 'yes'.

Another direction that future research could look into is Total Interpretive Structural Modelling (TISM). ISM interprets only the variables, whereas TISM interprets both variables and relationships in the digraph. Thus, the arrows in the graph are accommodated with statements on the relationships that are validated by experts. Moreover, in ISM all transitive links are eliminated, whereas in TISM, some important transitive links remain to provide clarity (Sushil, 2012).

Additionally, future research could focus on translating the variables and their interrelations to actual tools that can support decision-makers in assessing whether or not to adopt public cloud. Possible key criteria or scenarios can be thought out to further enhance this process.

6 Conclusion and reflection

In the final section of this study, the main research question will be answered. Then, the scientific implications will be discussed by revisiting the knowledge gaps that were identified in chapter 2.1. The section ends with a final reflection, in which policy recommendations are presented.

6.1 Main conclusion

The objective of this research was to investigate the landscape of variables that influence the decision to adopt public cloud technology. To achieve this objective, the following main research question was posed:

What is the interrelationship between variables that influence the decision to adopt public cloud computing within the Dutch public sector?

Throughout this study, methods have been employed to identify variables and analyse their interrelation. First, variables were identified using literature and Dutch official documents. Then, they were classified into two systems: incentives which would likely influence public cloud adoption decisions negatively (main perceived reasons to say 'no' to public cloud usage), i.e. the barriers, and incentives which would likely influence public cloud adoption decisions positively (main perceived reasons to say 'yes' to public cloud usage), i.e. the drivers. These systems were then analysed separately from each other.

Within the barrier system, it was found that a lack of knowledge had the strongest influence on incentives to say 'no' to public cloud usage, whereas inadequate regulations and government policy had the widest reach to influence these incentives. Moreover, the negative business case had the weakest influence on others in the system, and shared the lowest position for how many other variables it influenced with the variable internal resistance to change.

Within the driver system, it was found that the improved hard- and software had the strongest influence on incentives to say 'yes' to public cloud usage. The widest reach to influence other variables in the system was held by bigger knowledge market, ease of use and improved hard- and software. The driver with the weakest influence on others in the system was the governmental strategy, which also influenced the lowest number of other variables within the system.

These are only a few key results of this research, that shed light on the landscape of variables that influence the decision to adopt public cloud technology while acknowledging their possible interrelation.

Ultimately, the identification of these variables and recognition of the interrelationships between them can support decision-makers, managers, and policymakers to make informed and strategic

choices in relation to public cloud adoption. The results of this study can evolve into balanced guidelines and strategies that address challenges and opportunities in the current technology and policy landscape. A landscape that is evolving continuously, underlining the need for further research into the variables and their interrelations.

6.1.1 Scientific implications and contributions

When the existing body of scientific information with regard to cloud computing adoption in the public sector was analysed, three gaps were identified. Firstly, research was often not delineated to the Netherlands and therefore failed to capture geographically specific variables, such as legal or cultural characteristics. Secondly, authors who analysed the decision-making process of adopting cloud technology did not pay any attention to the interrelations between different variables. Thirdly, existing theories fell short in capturing the full scope of could computing adoption decisions, being either too general or not specific enough.

Geographical factors, such as culture or legal and regulatory frameworks have been identified as important by many authors (Gleeson & Walden, 2016) (Abied et al., 2022a) (Alenizi & Al-karawi, 2022). An example of this is a (lack of) existing IT infrastructure, which is identified as a major challenge to cloud adoption for developing countries but is far less recognised in other countries (Abied et al., 2022a) (Alenizi & Al-karawi, 2022). While no research about cloud adoption within the Dutch public sector specifically was done, it could be argued that the Netherlands falls under the institutional umbrella of the European Union. Directives of the EU largely determine the direction of the national legislation of its member states, making European research eligible to fill this knowledge gap (such as research by (Gleeson & Walden, 2016) and (Jones et al., 2019)). However, cultural factors can differ widely within Europe and influence adoption decisions as well (Alenizi & Al-karawi, 2022). This study therefore contributed to the existing body of knowledge by adding new insights to it that are based on official Dutch documents and reports, as well as on an analysis performed in the context of the Dutch public sector.

Existing studies that analysed variables influencing cloud computing adoption within the public sector have so far not acknowledged any interplay between variables (Assaf et al., 2021) [1]. However, several authors did define a hierarchy between the variables in terms of importance, using e.g. input of experts or Analytical Hierarchical Process (AHP) (Yoo & Kim, 2018). For the drivers (i.e. the incentives to say 'yes' to public cloud adoption within the Dutch public sector), the ability to be scale-able or having enough IT knowledge were identified as the most important variables to influence cloud computing adoption decisions (Abied et al., 2022b) (Mohammed & Ibrahim, 2015) (Ali et al., 2016). The results of this study showed that a bigger knowledge market, which generates enough IT knowledge and scalability, flexibility and agility both claim a high position within the system of other drivers (see figure 4.2. Thus, these results support previous findings and add to the literature by using a new method. In this sense, it could be argued that perceived important variables within the drivers' system correspond with those who influence the most other variables.

[1] Even in other sectors, only two examples of interrelation analysis were found (Choi et al., 2016) (Garg. & Stiller., 2015), that were either deemed two complex or did not include enough relevant variables

For the barriers (i.e. the incentives to say 'no' to public cloud adoption within the Dutch public sector), existing studies seemed to agree that data security concerns and risks were the most important variables within the barriers system (Jones et al., 2019) (King & Raja, 2012) (Hujran et al., 2019), whereas government regulations are categorised as of medium importance (Yoo & Kim, 2018) (Hsu et al., 2014). By using ISM Fuzzy MICMAC analysis, this study uncovered the complexity of the influence that governmental regulations and policies have on other factors. This result challenges researchers to reevaluate the importance of this variable on cloud computing adoption decisions within the public sector.

To address the third knowledge gap, variables that were identified in previous studies, that used different existing models such as TOE, TAM or DOI, were combined with variables found in policy documents and official reports supplemented by interviews with experts to form a list of relevant variables. Combining models has been done by previous authors, such as TOE and DOI by Abied et al., 2022a, or DOI and institutional theory by Pinheiro Junior et al., 2020. The aforementioned authors noted that there was not 'one' model accurate (enough) to capture all of the factors influencing adoption decisions, and therefore combined them. This study sought a different approach to bridge the gap. Referring to the multi-actor nature of the problem (described in 1.2), this study aimed to represent all of the actors (and their interactions) by cherry-picking the most frequently identified variables from multiple existing theories. For example, TOE can be used for the CSC, because this framework focuses mainly on influencing factors as seen from the organisational level of implementation or a new technology (Tornatzky et al., 1990). However, DOI or TAM are often used for exploration on the individual level of implementation, which could encompass variables that are important to citizens, who in turn (as end users) drive the motivations for the CSC (Abied et al., 2022b). Institutional theory generates factors that are driven or restricted by external pressure and relate to the policymakers, CSPs and CSCs (Jabbar, 2019). Policy documents, official reports and expert input generated variables that were important in the specific context of the problem.

All these, sometimes overlapping, models and frameworks have different starting points to establish which variables are important. This resulted in the identification of new variables, but still did not capture the interconnected nature of barriers and drivers as regards to cloud computing adoption decisions. Even though the decision is viewed from the perspective of the CSC, its decision is in essence influenced by variables (one could even state 'values' at this point) that are deemed more or less important by the other actors. It is therefore that the 'cherry-picking method' which was used in this study added to the existing literature by using a variety of different models that included (but were not limited to) organisational, technological, economic, and contextual dimensions. Despite the holistic view that ultimately resulted from this approach, its nature was exploratory rather than theory testing or building, although maybe this approach can provide some building blocks for this. It highlights the need for a more integrated model that incorporates the complex multi-actor nature of the problem to address the knowledge gap.

One aspect that has only been touched upon briefly in this study is the external pressure that 'forces' the migrator (CSC) to consider cloud adoption. Rather than shape the outcome of the decision (like the variables do), these pressures evoke a sense of urgency to drive or restrict cloud computing adoption decisions. A governmental strategy focused on cloud technology as an answer to pressure to innovate directly influences the decision to adopt cloud computing. However,

this does not fully encompass the external forces at play here. Although most variables identified in this study are technical in nature, some can be placed within the context of institutional literature. Institutional literature concerns itself with institutions as forces on individuals and organisations that are often derived from external (social) pressures and restrictions (Jabbar, 2019). Coercive pressures, which can result in sanctions if not followed, are included in variables such as Governmental strategy or Supplier strategy. Not complying with the governmental strategy might ultimately result in legal sanctions, while the supplier strategy, as described in section 4.1 could lead to the discontinuation of current IT practices. Furthermore, normative pressures related to social pressure on organisations to conform to certain norms that originate from professional or industry associations are for example included in a lack of standards or improving security and availability (Krell et al., 2016). If a certain standard is set or a norm is determined based on a certain level of security or availability, non-compliance is often morally not accepted. While previous studies have highlighted the importance of external pressures in general (Yoo & Kim, 2018) (Pinheiro Junior et al., 2020), this study contributed to the existing literature by (implicitly) examining these pressures within the public sector cloud adoption context. These insights can in turn help to close the institutional 'void', that results from technology advancements surpassing institutional advancements (Hajer, 2003).

In conclusion, this study contributed to the existing literature by empirically validating variables that are important in cloud computing adoption decisions within the Dutch public sector context. Furthermore, it introduced a comprehensive overview of the interrelationships between the variables. Not only did it confirm the significance of previously explored factors, such as the importance of knowledge enhancement or technological (hard- and software) improvement, but it also established the importance of under-explored ones, such as supplier and knowledge market dynamics. It addressed gaps in current theories by including different models and frameworks to identify variables and implicitly contributed to the understanding of institutional forces that influence cloud adoption decisions. This ultimately expanded and enriched the existing knowledge about cloud computing adoption, which encourages issue analysis and learning development.

6.2 Reflection

In the next several years, the Dutch Government will have to determine its position towards the use of public cloud computing within the Dutch public sector. A recent change in government-wide cloud policy marked a first step towards a possible transformation. A year after its introduction in 2022, this study investigated the decision landscape as it is today. In this reflection, practical implications are presented that explore the impact this research could have on decision-making. Conclusively, policy recommendations are presented that provide viable steps based on the research.

6.2.1 Decision making

An important aspect of decision-making is weighing benefits against costs or pros against cons. This research showed that variables in the decision-making process regarding cloud adoption can have complex interrelations. Within the Dutch (or maybe any) public sector, variables should not only be ranked on individual importance, but also be analysed based on the influence and number (and strength) of interrelations within the system. This will not only lead to more knowledge among researchers but also provide valuable insights for policymakers and various other

stakeholders. Making results visible for decision-makers, for instance that legacy dependence is mostly seen as an 'autonomous' factor, or that flexibility is ultimately linked to costs, helps them to create a well-considered plan of action for cloud adoption decisions. The study also addresses the dynamic environment of the problem, which underlines the critical role of research in shaping the future of cloud adoption practices. All this ensures that decision-makers remain responsive to evolving challenges and new opportunities within the Dutch public sector.

6.2.2 Recommendations

This thesis concludes with a translation of the main findings into actions the relevant stakeholders can take in the multi-actor system that was sketched in 1.2.

A lack of knowledge and *regulations and government policies* are key variables within the barrier system. Based upon these findings, knowledge development, especially *within* institutions that provide the rules and regulations, such as the government or parliament should be stimulated. Evidently, governmental agencies also came to this conclusion as several IT knowledge-creating projects such as traineeships or doctorates have been set up or expanded in the last year (BZK, 2023). Another example is the joining of the RADIO (translated from Dutch to English as the National Academy for Digitisation and Informatisation Government) to the BZK (Ministry of the Interior and Kingdom Relations) in order to train civil servants in all fields on IT-related subjects.

This bottom-up approach of educating the next generation of researchers and civil servants in general will eventually lead to knowledgeable managers and policymakers, that can assess cloud (or other digital) decisions appropriately. Undoubtedly, this approach will result in more knowledge overall, but the process might take years to yield the desired result. In addition to this, many experts who participated in this study observed an inverse knowledge-responsibility trend. This trend indicated that the people with the most responsibility (e.g. top officials, policymakers or directors) did not always possess the required knowledge that was necessary to make informed decisions. Decisions often were delegated to technical teams with more knowledge, but these teams did not always possess the authority to convince the people with the most responsibility of their conclusions. This phenomenon might find its origins within the hierarchical nature of governmental agencies. However, the cloud computing market is advancing quickly, and it is crucial to acknowledge the importance of authoritative leaders who are highly skilled in cloud technology, or even IT-related fields in general. These leaders, forming a 'cloud authority' can help to make sure that cloud adoption within the Dutch public sector will not be bogged down.

This 'cloud authority' of knowledgeable top official(s) could address the barriers (see 2.4) by advising on rules and regulations and promoting collaboration, (inter-organisational) knowledge sharing and standardisation. It could create governance frameworks to address the fear of losing control and advise on security concerns. Such a cloud authority should preferably be central and independent, therefore surpassing the *segmented structure of the public sector* as identified in 4.1. Furthermore, it can direct independent research on incentives to say 'yes' to the cloud (i.e. the drivers), as there are currently no specific (official Dutch) reports on this. Most of these 'yes' incentives are provided by the CSP which seeks to gain a competitive advantage, making it difficult to base a well-balanced decision on them.

However, will appointing a cloud authority help to navigate the Dutch sector through the complex cloud landscape? While it certainly would bring benefits, it is essential to see this problem in a broader European Union context. Collaborating with other European countries can bring about numerous advantages, such as international knowledge sharing, standardisation and more economies of scale. As the world gets more and more interconnected, tackling the complex cloud landscape collectively can lead to a more robust and unified approach where common values, such as digital sovereignty, compliance, availability and security are paramount. A start with these collaborative efforts has already been made but it is moving very slowly. It was only on the 15th of July 2023 that the first objectives of the 'European industrial technology road map for the next-generation cloud-edge' were published by the European Alliance for Industrial Data, Edge and Cloud [2] (European Alliance for Industrial Data & Cloud, 2023). Therefore a rapid proposal from the European Commission to install a supranational cloud authority to be discussed in the European Parliament and accepted by all EU member states seems highly desirable. Top officials from the different member states with expert knowledge can speed up the process by forming opinions that reflect their nation's needs while being able to assess what is possible in the cloud. This could result in the development of a uniform European cloud strategy that is not hindered by a lack of knowledge.

To summarise the recommendations: based upon the findings of this study, there is an urgent need for knowledge development at different levels of government. Currently, knowledge development already takes place but especially among younger generations or in technical teams that have relatively low responsibility and little power to implement policies. To address the imminent need for IT-skilled ánd top-level decision-makers, the establishment of a 'cloud authority' is proposed, which consists of top official(s) who have expert cloud knowledge and who can develop a policy with clear objectives, a substantial budget and fixed deadlines to be decided upon swiftly by well-informed politicians. This cloud authority can also initiate research into public sector-specific drivers, while simultaneously having enough authority to advise other top officials on cloud-related matters. All EU member states should have their own representative in the EU-Cloud Authority (EUCLAUT) focusing on agile and well-balanced decision-making.

In conclusion, this study supports decision-makers, managers, and policymakers in making informed and strategic choices in relation to public cloud adoption. The recommendations outline possible next steps to be taken, but the government should always look critically at what is needed to realise these steps and cloud adoption in general but also consider adequate alternatives such as the improvement of on-premises structures or processing data closer to the source (edge-computing) which could reduce the need for cloud resources.

[2]The Alliance is formed by organisations that are of 'significant relevance to the provision of highly secure cloud and data processing' and have a legal representative within the EU (European Alliance for Industrial Data & Cloud, 2023)

Bibliography

Abied, O., Ibrahim, O., Kamal, S. N.-I. M., Alfadli, I. M., Binjumah, W. M., Ithnin, N., & Nasser, M. (2022a). Probing determinants affecting intention to adopt cloud technology in e-government systems. *Sustainability*, *14*(23). https://doi.org/10.3390/su142315590

Abied, O., Ibrahim, O., & Mat Kamal, S. N.-I. (2022b). Adoption of cloud computing in e-government: A systematic literature review. *Pertanika Journal of Science and Technology*, *30*(1), 655 –689. https://doi.org/10.47836/PJST.30.1.36

Alenizi, A. S., & Al-karawi, K. A. (2022). Cloud computing adoption-based digital open government services: Challenges and barriers. *Lecture Notes in Networks and Systems*, *216*, 149 –160. https://doi.org/10.1007/978-981-16-1781-2_15

Ali, O., Soar, J., & Yong, J. (2016). An investigation of the challenges and issues influencing the adoption of cloud computing in australian regional municipal governments [Special Issues on Security and Privacy in Cloud Computing]. *Journal of Information Security and Applications*, *27-28*, 19–34. https://doi.org/https://doi.org/10.1016/j.jisa.2015.11.006

Alonso, J., Escalante, M., & Orue-Echevarria, L. Transformational cloud government (tcg): Transforming public administrations with a cloud of public services [All Open Access, Gold Open Access]. In: *97*. All Open Access, Gold Open Access. 2016, 43 –52. https://doi.org/10.1016/j.procs.2016.08.279.

Amrina, U., & Oktora, A. (2020). Analysis of lean and green drivers for sustainable cosmetics smisusing interpretive structural modelling (ism). *International Journal of Engineering Research and Advanced Technology*, *06*, 08–16. https://doi.org/10.31695/IJERAT.2020.3614

Assaf, A., Hamsir, A. W. I., & Muhammad, M. Benefits and risks of cloud computing in e-government tasks: A systematic review. In: *328*. 2021. https://doi.org/10.1051/e3sconf/202132804005.

Attri, R., Dev, N., & Sharma, V. Interpretive structural modelling (ism) approach: An overview. In: 2013.

Aziz, M. A., Abawajy, J., & Chowdhury, M. The challenges of cloud technology adoption in e-government. In: 2013, 470 –474. https://doi.org/10.1109/ACSAT.2013.98.

Bashir, H., Hamid, S. A.-k., Ojiako, U., Haridy, S., & Shamsuzzaman, M. An integrated ism-fuzzy micmac approach for modeling and analyzing information flows among product development project activities. In: *2022 advances in science and engineering technology international conferences (aset)*. 2022, 1–6. https://doi.org/10.1109/ASET53988.2022.9735013.

Bharosa, N. (2022). The rise of govtech: Trojan horse or blessing in disguise? a research agenda. *Government Information Quarterly*, *39*(3), 101692. https://doi.org/https://doi.org/10.1016/j.giq.2022.101692

Bolanos, R., Fontela, E., Nenclares, A., & Pastor, P. (2005). Using interpretive structural modelling in strategic decision-making groups. *Management Decision*, *43*, 877–895. https://doi.org/10.1108/00251740510603619

BZK. (14-01-2022). Gdi-meerjarenvisie 2022-2026 [[Online; accessed 12-July-2023]].

BZK. (2023). *Rijks i-doctoraatsprogramma*. Retrieved August 30, 2023, from https://www.rijksorganisatieodi.nl/i-partnerschap/rijks-i-doctoraatsprogramma

Choi, C.-R., Jeong, H.-Y., Park, J. H., Jang, H. J., & Jeong, Y.-S. (2016). Relative weight comparison between virtual key factors of cloud computing with analytic network process [Cited by: 3]. *Journal of Supercomputing*, *72*(5), 1694 – 1714. https://doi.org/10.1007/s11227-014-1311-x

Dash, S., & Pani, S. K. E-governance paradigm using cloud infrastructure: Benefits and challenges. In: *85*. 2016, 843 –855. https://doi.org/10.1016/j.procs.2016.05.274.

Daylami, N. (2015). The origin and construct of cloud computing. *International Journal of the Academic Business World*, *9*(2), 39–45.

Deshmukh, A., & Mohan, A. (2017). Analysis of indian retail demand chain using total interpretive modeling. *Journal of Modelling in Management*, *12*, 00–00. https://doi.org/10.1108/JM2-12-2015-0101

Dubey, R., & Ali, S. S. (2014). Identification of flexible manufacturing system dimensions and their interrelationship using total interpretive structural modelling and fuzzy micmac analysis. *Global Journal of Flexible Systems Management*, *15*, 131–143.

Dubey, R., & Singh, T. (2015). Understanding complex relationship among jit, lean behaviour, tqm and their antecedents using interpretive structural modelling and fuzzy micmac analysis. *The TQM Journal*, *27*, 42–62. https://doi.org/10.1108/TQM-09-2013-0108

Elena, G., & Johnson, C. (2015). Factors influencing risk acceptance of cloud computing services in the uk government. *International Journal on Cloud Computing: Services and Architecture*, *5*. https://doi.org/10.5121/ijccsa.2015.5301

European Alliance for Industrial Data, E., & Cloud. (2023, July 15). *European industrial technology roadmap for the next-generation cloud-edge*. Retrieved August 30, 2023, from https://ec.europa.eu/newsroom/dae/redirection/document/97129

Garg., R., & Stiller., B. Factors affecting cloud adoption and their interrelations. In: *Proceedings of the 5th international conference on cloud computing and services science - closer*. INSTICC. SciTePress, 2015, 87–94. ISBN: 978-989-758-104-5. https://doi.org/10.5220/0005412300870094.

Gartner. (2022). Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly 600 Billion in 2023 [[Online; accessed 30-March-2023]].

Gleeson, N., & Walden, I. (2016). Placing the state in the cloud: Issues of data governance and public procurement. *Computer Law Security Review*, *32*(5), 683–695. https://doi.org/https://doi.org/10.1016/j.clsr.2016.07.004

Ha, L. (2022). Are digital business and digital public services a driver for better energy security? evidence from a european sample. *Environmental Science and Pollution Research*. https://doi.org/10.1007/s11356-021-17843-2

Hajer, M. (2003). Policy without polity? policy analysis and the institutional void. *Policy Sciences*, *36*, 175–195. https://doi.org/10.1023/A:1024834510939

Halvorsen, T., Hauknes, J., Miles, I., & Røste, R. (2005). Innovation in the public sector on the differences between public and private sector innovation.

Hartholt, S. (2022, February 21). *Tweede kamer: Kabinet moet cloudbeleid heroverwegen en kiezen voor europees alternatief*. Retrieved September 15, 2023, from https://www.agconnect.nl/maatschappij/juridisch/tweede-kamer-kabinet-moet-cloudbeleid-heroverwegen-en-kiezen-voor-europees-alternatief

Hsu, P.-F., Ray, S., & Li-Hsieh, Y.-Y. (2014). Examining cloud computing adoption intention, pricing mechanism, and deployment model. *International Journal of Information Management*, *34*(4), 474 – 488. https://doi.org/10.1016/j.ijinfomgt.2014.04.006

Hujran, O., Al-Lozi, E., Al-Debei, M., & Maqableh, M. (2019, January). Challenges of cloud computing adoption from the toe framework perspective. https://doi.org/10.4018/978-1-5225-8176-5.ch066

IBM. (2022). *What is data security*. Retrieved January 17, 2023, from https://www.ibm.com/topics/data-security

ICT-toetsing, H. A. (2021). Overzicht toetsaspecten risicogebieden [[Online; accessed 17-May-2023]].

Jabbar, A. A. (2019). Studying the effect of institutional pressures on the intentions to continue green information technology usage.

Jones, S., Irani, Z., Sivarajah, U., & Love, P. E. D. (2019). Risks and rewards of cloud computing in the uk public sector: A reflection on three organisational case studies. *Information Systems Frontiers*, *21*(2), 359–382. www.scopus.com

Junior, J., Salonitis, K., & Brintrup, A. (2021). Key enablers for the evolution of aerospace ecosystems. *Journal of Aerospace Technology and Management*, *13*. https://doi.org/10.1590/jatm.v13.1225

Kamble, S., Gunasekaran, A., & Sharma, R. (2018). Analysis of the driving and dependence power of barriers to adopt industry 4.0 in indian manufacturing industry. *Computers in Industry*, *101*, 107–119. https://doi.org/10.1016/j.compind.2018.06.004

Kandasamy, F., Kandasamy, W., Smarandache, F., & Ilanthenral, K. (2007). *Elementary fuzzy matrix theory and fuzzy models for social scientists*. Multimedia Larga. https://books.google.nl/books?id=G5mNvsQtOiUC

Khan, U., & Haleem, A. (2012). Smart organisations: Modelling of enablers using an integrated ism and fuzzy-micmac approach. *Int. J. of Intelligent Enterprise*, *1*, 248 –269. https://doi.org/10.1504/IJIE.2012.052556

Khatwani, G., Singh, S. P., Trivedi, A., & Chauhan, A. (2015). Fuzzy-tism: A fuzzy extension of tism for group decision making. *Global Journal of Flexible Systems Management*, *16*, 97–112.

King, N. J., & Raja, V. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law Security Review*, *28*(3), 308–319. https://doi.org/https://doi.org/10.1016/j.clsr.2012.03.003

Kotka, T., Johnson, B., Cebul, T., Lovosevic, L., & Liiv, I. (2016, August). E-government services migration to the public cloud: Experiments and technical findings. https://doi.org/10.1007/978-3-319-44159-7_5

Krell, K., Matook, S., & Rohde, F. (2016). The impact of legitimacy-based motives on is adoption success: An institutional theory perspective. *Information Management*, *53*(6), 683–697. https://doi.org/https://doi.org/10.1016/j.im.2016.02.006

Kuiper, E., Van Dam, F., Reiter, A., & Janssen, M. Factors influencing the adoption of and business case for cloud computing in the public sector [Cited by: 2]. In: Cited by: 2. 2015. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84966683224&partnerID=40&md5=cf2223d1b0acd0e67acc5058f4dd6b61

Lee, S. M., Hwang, T., & Choi, D. (2012). Open innovation in the public sector of leading countries. *Management decision*.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — the business perspective. *Decision Support Systems*, *51*(1), 176–189. https://doi.org/https://doi.org/10.1016/j.dss.2010.12.006

Mell, P., & Grance, T. (2011). Nist special publication 800-145: The nist definition of cloud computing. *Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD*, 20899–8930.

MIDO-kader. (2022). Mido-kader [[Online; accessed 12-July-2023]].

Mohammed, F., Ibrahim, O., Nilashi, M., & Alzurqa, E. (2017). Cloud computing adoption model for e-government implementation. *Information Development*, *33*(3), 303–323.

Mohammed, F., & Ibrahim, O. B. (2015). *Drivers of cloud computing adoption for e-government services implementation* [Cited by: 0]. https://doi.org/10.4018/978-1-4666-9466-8.ch038

Mutkoski, S. National cloud computing legislation principles: Guidance for public sector authorities moving to the cloud. In: 2015, 404 –409. https://doi.org/10.1109/IC2E.2015.104.

Nanos, I., Manthou, V., & Androutsou, E. Cloud computing adoption decision in e-government. In: 2019, 125 –145. https://doi.org/10.1007/978-3-319-95666-4_9.

Pfohl, H.-C., Gallus, P., & Thomas, D. (2011). Interpretive structural modeling of supply chain risks. *International Journal of Physical Distribution Logistics Management*, *41*, 839–859. https://doi.org/10.1108/09600031111175816

Pinheiro Junior, L., Alexandra Cunha, M., Janssen, M., & Matheus, R. Towards a framework for cloud computing use by governments: Leaders, followers and laggers. In: *The 21st annual international conference on digital government research*. dg.o '20. Seoul, Republic of Korea: Association for Computing Machinery, 2020, 155–163. ISBN: 9781450387910. https://doi.org/10.1145/3396956.3396989.

Qian, L., Luo, Z., Du, Y., & Guo, L. Cloud computing: An overview (M. G. Jaatun, G. Zhao, & C. Rong, Eds.). In: In *Cloud computing* (M. G. Jaatun, G. Zhao, & C. Rong, Eds.). Ed. by Jaatun, M. G., Zhao, G., & Rong, C. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, 626–631.

Rijksoverheid, N. (2022, August 29). *Werken 'in de cloud' wordt mogelijk voor rijksoverheid*. Retrieved December 22, 2022, from https://www.rijksoverheid.nl/actueel/nieuws/2022/08/29/werken-in-de-cloud-wordt-mogelijk-voor-rijksoverheid

Sage, A. P. (1977). *Methodology for large-scale systems*. McGraw-Hill College.

Saxena, J., Sushil, P., & Vrat, P. (1992). Scenario building: A critical study of energy conservation in the indian cement industry. *Technological Forecasting and Social Change*, *41*, 121–146. https://doi.org/10.1016/0040-1625(92)90059-3

Schuman, S. P. (2002). Believe in doubt. *Group Facilitation: A Research and Applications Journal*, *4*(1).

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. john wiley & sons.

Sindhwani, R., & Malhotra, V. (2016). Modelling and analysis of agile manufacturing system by ism and micmac analysis. *International Journal of System Assurance Engineering and Management*, *8*. https://doi.org/10.1007/s13198-016-0426-2

Smania, G. S., de Sousa Mendes, G. H., Godinho Filho, M., Osiro, L., Cauchick-Miguel, P. A., & Coreynen, W. (2022). The relationships between digitalization and ecosystem-related capabilities for service innovation in agricultural machinery manufacturers. *Journal of Cleaner Production*, *343*, 130982. https://doi.org/https://doi.org/10.1016/j.jclepro.2022.130982

Sushil, P. (2012). Interpreting the interpretive structural model. *Global Journal of Flexible Systems Management*, *13*. https://doi.org/10.1007/s40171-012-0008-3

Tewarie, W., & van der Veen, J. (2023). Clouddiensten BIO Thema-uitwerking [[Online; accessed 30-March-2023]].

Tornatzky, L., Fleischer, M., & Chakrabarti, A. (1990). *The processes of technological innovation*. Lexington Books. https://books.google.nl/books?id=EotRAAAAMAAJ

Tsohou, A., Lee, H., & Irani, Z. (2014). Innovative public governance through cloud computing: Information privacy, business models and performance measurement challenges. *Transforming Government: People, Process and Policy*, *8*(2), 251 –282. https://doi.org/10.1108/TG-09-2013-0033

van Dijk, J., & Jacobs, B. (2022). Opinie: Onze overheid moet haar kostbare data niet klakkeloos uitleveren aan google en amazon. *de Volkskrant*. Retrieved August 10, 2023, from https://www.volkskrant.nl/columns-opinie/opinie-onze-overheid-moet-haar-kostbare-data-niet-klakkeloos-uitleveren-aan-google-en-amazon~b57cb834/

van Donge, W., Bharosa, N., & Janssen, M. F. W. H. A. Future government data strategies: Data-driven enterprise or data steward? exploring definitions and challenges for the government as data enterprise. In: *The 21st annual international conference on digital government research*. dg.o '20. Seoul, Republic of Korea: Association for Computing Machinery, 2020, 196–204. ISBN: 9781450387910. https://doi.org/10.1145/3396956.3396975.

Warfield, J. (1994). *A science of generic design: Managing complexity through systems design*. Iowa State University Press. https://books.google.nl/books?id=e-seAQAAIAAJ

Warfield, J. N. (1974). Developing interconnection matrices in structural modeling. *IEEE Transactions on Systems, Man, and Cybernetics*, *SMC-4*(1), 81–87. https://doi.org/10.1109/TSMC.1974.5408524

Wolfsen, A. (2022, November 11). *Brief over rijksbreed cloudbeleid 2022*. The Hague.

Yoo, S.-K., & Kim, B.-Y. (2018). A decision-making model for adopting a cloud computing system. *Sustainability*, *10*(8). https://doi.org/10.3390/su10082952

Zimmermann, H.-J. (1996). Fuzzy control. *Fuzzy set theory—and its applications* (pp. 203–240). Springer Netherlands. https://doi.org/10.1007/978-94-015-8702-0_11

Zwattendorfer, B., Stranacher, K., Tauber, A., & Reichstädter, P. (2013). Cloud computing in e-government across europe a comparison. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8061 LNCS*, 181 –195. https://doi.org/10.1007/978-3-642-40160-2_15

Appendix A

Preliminary literature review

In this literature review, the state-of-the-art challenges related to cloud computing technology and the government are evaluated. This evaluation will provide the base for this master's thesis research which will explore how cloud technology will influence the Dutch government, and identify challenges that will arise by using cloud technology within the current governmental ICT - landscape. After presenting the keywords and selection criteria that were used to find relevant research, the findings will be presented. After that, the most important conclusions will be presented and the gap in the literature will be identified.

Challenges of cloud computing

In this section, the implications of cloud computing and its use within the Dutch public sector will be discussed. First the challenges will be discussed, followed by an extensive overview of the benefits and risks.

Overview

In recent years, cloud computation is gaining in popularity. The enormous benefits that cloud computing can bring in terms of scalability and cost savings have made it very attractive for a lot of companies (Aziz et al., 2013)(Mutkoski, 2015). For entities in the public sector, especially in the government, cloud adoption has progressed a lot slower (Zwattendorfer et al., 2013). In this section, findings in regard to the current challenges are grouped per main topic. The research that is presented includes both qualitative, quantitative and mixed methods research. Methods used by (Ali et al., 2016) for example were a systematic literature review and in depth interviews were used, and (Jones et al., 2019) combined a literature review with three case studies. Some of the authors first introduced the term e-government, which (Mutkoski, 2015) defines as "the government's use of information and communication technologies for providing electronic public services to citizens, the government itself, public officers, politicians, businesses, etc." As stated in the selection criteria, no distinction will be made in this literature review, as e-government services can be viewed as a part of government services in general.

Security and Privacy

When talking about the use of cloud computing within governmental bodies, security concerns are very often the first reaction and possibly even the main challenge (Dash & Pani, 2016). One of the challenges found in the research was data security. Data security can be defined as protecting data from unauthorised access, corruption, or theft (IBM, 2022). The cloud computing model characteristic of using shared resources and components will increase the risk of unauthorised access to data by other subscribers (e.g. hackers) which could potentially exploit vulnerabilities in the cloud environment (King & Raja, 2012) (Jones et al., 2019)(Ali et al., 2016). Additionally, research by (King & Raja, 2012) suggests that the increased system complexity will provide a larger 'area' where systems are vulnerable to hackers and that the internet-delivery of public cloud services exposes government services to new network threads. Furthermore, fulfilling the requirement of

a stable internet connection for access to cloud computing resources is identified as a challenge on its own (Alenizi & Al-karawi, 2022).

Other than these technical security challenges, policies that ensure data protection are needed in order to guarantee data-security during the cloud transformation of the public sector and identify the deficiency of protective facilities in the public sector (Tsohou et al., 2014).

Concerns relating to privacy refer to who is allowed to access data. These concerns form one of the biggest challenges for European governments that are interested in using the services of commercial public cloud providers. Since the biggest cloud providers are mainly situated in the US, external control by the cloud service provider can pose severe security and privacy threats. Updating current regulations to limit the trans-border data flow is therefore seen as a relevant challenge by many researchers (Nanos et al., 2019) (King & Raja, 2012).

Limiting the trans border data flow is one way to answer to privacy and security concerns, but it can be a very lengthy and (costly) process to determine which data can be stored. Current IT processes that handle both sensitive and insensitive data need to be redesigned and eventually both public cloud and on-premise IT systems need to be managed. One could pose the question if this wouldn't eventually lead to even more complexity and costs, undoing the cost-reduction argument to move to the cloud in the first place. Research by (Ali et al., 2016) indicated that 33 per cent of cloud users are concerned about the data storage location, because the location of the servers will decide under which policy the stored data is held. He argues that the lack of clarity about data storage cloud providers and consumers makes it more difficult to create policies that would be better tailored to data storage in the cloud, instead of just limiting the trans-border data flow in general. More research stresses the need for a harmonised set of guidelines should be formed for the use of personal data (Tsohou et al., 2014), and show that the lack of user control in cloud usage remains a threat to privacy (Jones et al., 2019). Additionally, business continuity strategies, which are e.g. supported by good agreements and back-ups, should be in place to ensure the continuity of government services if cloud services fail. (Aziz et al., 2013).

Provider dependency, data portability and standardization

Choosing the right cloud provider is recognised as a challenge by many articles (Alonso et al., 2016) (Ali et al., 2016). Other than the fact that the location of the cloud provider is important due to legal restrictions for security and privacy reasons, location is important in relation to latency and high availability (Alonso et al., 2016). Research by (Ali et al., 2016) discussed the fact that government agencies in some areas struggle to choose the cloud provider which best suits their needs, because there are no cloud providers that offer a sufficient level of services. However, in areas where cloud providers do provide a high level of technological maturity, they often form a heterogeneous landscape(Zwattendorfer et al., 2013). Consequently, the threat of a vendor lock-in arises. Vendor lock-in occurs if the cost to switch from the current to an alternative cloud provider is so high, e.g. due to training or data transfer cost, that even though the alternative cloud provider offers a better pricing or technological option, the consumer will stay at the initial provider. The importance of vendor lock-in avoidance is argued by (Zwattendorfer et al., 2013) and (Alonso et al., 2016).

A challenge related to vendor lock-in is the lack of data portability. Data portability is the ability to transfer data across different cloud providers and services. Ensuring data portability can help to ensure limited cloud provider dependence and avoid vendor lock-in and allow for a wider choice of cloud providers. Data portability is identified by many researchers as a challenge (Nanos et al., 2019) (Kotka et al., 2016). A lack of interoperability [1] and standardization also affects the data portability and increases cloud provider dependence (**Alenizi2022149**). However, (Mutkoski, 2015) argues that, even though standardization should not be discouraged, the measured service provided by the cloud can be used as an advantage that wouldn't require such strong standardization in the first place. The challenge here can be seen as not to standardize the governmental departments, but allowing and ensuring that governmental authorities have the option to choose which cloud structure (and provider) fits their specific needs. Additionally, an increased standardization will ensure compliance-compatibility with existing systems (Nanos et al., 2019), research by (Kotka et al., 2016) states that standardization across government services will additionally ease operational management.

Interoperability, integration and legacy

Many authors defined challenges related to a lack of integration and interoperability between the different information systems of the government. Different departments of the government use different databases, different programming languages and have a different Legacy information system, that they are dependent on. (Mutkoski, 2015) (Aziz et al., 2013) (Nanos et al., 2019) [2]. There is a lack of interconnection between the different departments and a lack of common architecture, as well as an absence of common standards (Nanos et al., 2019). The lack of common standards is described in the previous paragraph, so this section will mainly focus on the integration and interoperability aspects.

When migrating to the cloud, integration of current systems with the proposed new cloud system is seen as a challenge by governmental authorities. Integration in this sense means the level that the current on-premise computing resources can interact with the 'new' cloud infrastructure. Lack of integration can result in a failure to yield the benefits that cloud computing can provide, and in adoption failure in general (Ali et al., 2016).

Interoperability relates to the fact that different components are actually using the same 'communicating' language. This can be done by enforcing the same standards or framework. The need for a common regulatory framework for best practices, at legal, technical and operational level is explored in (Alonso et al., 2016). Research by (Alenizi & Al-karawi, 2022) also relates the lack of common standards to interoperability and claims that consumers of cloud computing services should be able to migrate among cloud service suppliers with a minimum of threat and expense(Alenizi & Al-karawi, 2022).

Organisational, economical and social challenges

Research by (Halvorsen et al., 2005) suggests that private sector companies are more able to adapt to the cloud faster because they are able to change their organisational structure in a flexible way.

[1] Described in section 3.4

[2] *Legacy* is denoted by the Oxford dictionary as: "denoting or relating to software or hardware that has been superseded but is difficult to replace because of its wide use."

Public cloud companies provide new services and updates almost daily and are ever-changing in nature. The dynamic nature of this technology suggests that an agile way of working enhances a successful implementation of cloud technology. Research by (Kotka et al., 2016) found that using an agile approach to application building ensures a quicker response to threats.
Since governmental bodies are usually characterised by bureaucracy, rigid structures, and a low degree of innovation adoption (Nanos et al., 2019), one could argue that cloud technology would not be compatible. However, studies have found that within Europe, cloud computation has been used by many governments in various forms and deployment models (Zwattendorfer et al., 2013). (Mutkoski, 2015) argues that the adoption of cloud computing itself makes the government more agile in responding to public needs.

Even though much research indicates that the adoption of cloud computing technology within the government will result in a cost reduction and view it as one of the benefits of transitioning to the technology (Mutkoski, 2015), some authors consider cost as one of the challenges. This can be related to the cost of training and hiring relevant IT personnel, or higher start-up costs (Ali et al., 2016). However, (Ali et al., 2016) argue in the same article that the higher start-up costs are only perceived by consumers and not backed up by the actual numbers. Taking this into account, perceived high start-up costs can still count as a challenge for governmental bodies to adopt cloud technology and might fall into the category 'lack of awareness' that will be analysed in the next paragraph.

The lack of awareness and understanding is highlighted as a challenge by many authors. Research by (Alenizi & Al-karawi, 2022) found that there is a lack of orientation campaigns to endorse digital government and cloud use. This can result in a lack of national vision to stimulate digital growth in general and a lack of motivation to innovate by employees in the public sector (Nanos et al., 2019). Cloud computing, just like any other innovation, needs enough 'push' to be successful, and it is therefore very important that the motivation to innovate does not diminish, due to lack of understanding. However, research by (Ali et al., 2016) indicates that "the willingness of the stakeholders to accept the new way of doing things" is seen as a difficulty within the government, which can be supported by the definition of the government as a bureaucratic, rigid structure with a low degree of innovation adoption (Nanos et al., 2019).

Other than awareness and motivation to innovate, the actual lack of 'hard skill' IT knowledge present in the current governmental employee pool could form an obstruction to successful implementation. The lack of IT-skilled personnel within the governmental authorities, and the difficulty of obtaining enough IT-skilled personnel, is highlighted in research done by (Aziz et al., 2013). Aside from the employees, the top management that is in the end responsible for deciding to adopt cloud technology, is often lacking sufficient background knowledge in IT to make an accurate decision and consequently fails to offer sufficient tools that help the successful adoption of cloud computing (Ali et al., 2016).

The last challenge that was identified within the existing literature was a lack of trust. This lack of trust was not only ascribed to the cloud computing technology itself, but in a wider range to the internet and government electronic services. Citizens fear a lack of protection by the government (Alenizi & Al-karawi, 2022). However, one author argues that providing more governmental services online, which is established by using cloud technology, can increase transparency and stimulate trust (Aziz et al., 2013). Trust is also an important aspect between the governmental

authority and the cloud provider (Jones et al., 2019). Many aspects related to the security and privacy of data are handled by the cloud provider so it is of important that there is sufficient trust between the government and the cloud provider.

Conclusions

Cloud computing is gaining in popularity. Due to rapid development, the risks that used to be associated with its use are decreasing. Advantages such as cost reduction, flexibility and scaleability made cloud computing technology already widely adopted by companies in the private sector. The adoption did only take place to a certain extent by organisations in the public sector, due to security and other concerns Zwattendorfer et al., 2013. In the Netherlands, the same trend can be observed by the fact that governmental authorities could, until recently legally only use private (on-premise) cloud computing resources. However, recent developments have led the Dutch government to reevaluate its cloud policy and allow the use of commercial cloud services. This change in cloud policy prompted my research to identify current challenges related to commercial (public) cloud adoption in the government.

In this literature review the state-of-the-art challenges related to cloud computing technology and its adoption (and implementation) by governments are evaluated. After analyzing the literature, numerous challenges were identified. Security-related challenges, that aim to limit unauthorized access, can be distinguished into technical challenges, e.g. related to the ease at which hackers can access the data, as well as non-technical challenges, such as data protection policy formation. Policies can also help in the mitigation of privacy concerns, either by limiting the trans-border data flow or by allowing tailored cloud usage by the government. Challenges related to provider dependency and vendor lock-in can possibly be overcome by tackling the challenges posed by ensuring data portability and interoperability and striving for standardisation across governmental IT infrastructures. A lack of awareness and understanding of cloud computing technology and how the government can benefit from its use can result in a failure of adoption. Acquiring the knowledge and personnel needed should therefore be a key priority for governmental authorities that consider cloud transformation. Lastly, the importance of realising trust between citizens and government, and government and cloud provider is established as a requirement for the successful adoption and implementation of cloud computing technology.

The main goals of this literature review were to understand the state-of-the-art and to determine the existence of research gaps. The research gaps will be described in this section. The first research gap was found when my search began, as there were only limited authors who wrote about cloud adoption challenges within the Dutch government. Taking into account that cloud computing is a very new technology and has only recently become 'mature enough' to use by the public (and governmental) sector, and that the Netherlands is a small geographical area, this gap is not surprising. However, since many private sector companies in the Netherlands have already successfully adopted cloud technology (Rijksoverheid, 2022), and the regulations around the use of commercial (public) cloud computing technology has recently changed, the need for research to support cloud adoption decisions is increasing.

The second gap emerged from the fact that many intertwining challenges have been identified within the literature, but no authors fully developed these challenges into a comprehensive assessment framework. Many did note that the goal of their research was to aid managers in their

decision to adopt cloud technology, but no research has resulted in an assessment framework that can be used in practice. This could be a problem that I could try to solve in my master's thesis. A start for such a framework can be made by understanding how challenges that were presented in this literature review relate to each other and recognising any interdependence. Additionally, future research is needed to identify other factors, such as benefits, risks, or existing digital infrastructure, that influence the decision of governmental bodies to adopt cloud computing technology.

Appendix B

Keywords and citations

Search term	Hits	Number of articles used	Citation
TITLE-ABS-KEY ("cloud " drivers "public sector")	10	1	(Ha, 2022)
TITLE-ABS-KEY ("cloud computing" "adoption" "factors")	1,056	5	(Hsu et al., 2014), (Hujran et al., 2019), (Kotka et al., 2016), (Mutkoski, 2015), (Qian et al., 2009)
TITLE-ABS-KEY ("cloud computing" "barriers" "government")	64	1	(Alenizi & Al-karawi, 2022)
TITLE-ABS-KEY ("cloud computing" "challenges" "government")	534	5	(Abied et al., 2022b), (Ali et al., 2016), (Mohammed et al., 2017) (Alonso et al., 2016), (Aziz et al., 2013), (Nanos et al., 2019)
TITLE-ABS-KEY ("cloud computing" "europe" "challenge")	65	1	(King & Raja, 2012)
TITLE-ABS-KEY ("cloud computing" "europe" "public sector")	11	2	(Zwattendorfer et al., 2013) (Kuiper et al., 2015)
TITLE-ABS-KEY ("cloud computing" "government" "factors")	327	1	(Pinheiro Junior et al., 2020) (Mohammed & Ibrahim, 2015)
TITLE-ABS-KEY ("cloud computing" "government" "risks")	282	3	(Assaf et al., 2021), (Jones et al., 2019), (Elena & Johnson, 2015)
TITLE-ABS-KEY ("cloud computing" "public sector" "challenge")	72	1	(Tsohou et al., 2014)
TITLE-ABS-KEY ("cloud computing" "drivers" "public sector")	6	1	(Abied et al., 2022a)
TITLE-ABS-KEY ("innovation" "public sector" "factors")	808	2	(Halvorsen et al., 2005), (Lee et al., 2012) (Gleeson & Walden, 2016)
Found via snowballing		1	(Marston et al., 2011) (found in article (Hsu et al., 2014)

Non scientific sources	**Citation**
BIO	(Tewarie & van der Veen, 2023)
AC-ICT	(ICT-toetsing, 2021)
GDI	(BZK, 14-01-2022)
Rijksbreed cloudbeleid 2022	(Rijksoverheid, 2022)

Appendix C

Variable aggregation

Opportunities	Driver
Ability to launch new businesses rapidly	Scalability, flexibility and agility
Accelerated deployment of new IT capabilities	Bigger knowledge market
Access to new tools and services to accelerate business innovation	Improved hard- and software, Scalability, flexibility and agility, Improved security and availability
Accounting and tax implications of a shift from OPEX to CAPEX	Low and flexible cost
Achieve business benefits by changing the way we operate	Scalability, flexibility and agility, Improved integration and interoperability
Cloud improves analytics and insights by integrating data across silos	Improved integration and interoperability internally and externally
Cloud migration can help reduce high licensing costs	Low and flexible cost
Cloud reduces the technology gap (“the technical debt”) that arises as systems near end of life	Improving security and availability
Empower talent in new, more creative ways	Bigger knowledge market
Greater business flexibility, scalability and agility	Scalability, flexibility and agility
Identify and target better candidates	Bigger knowledge market
Improved business agility	
Increased speed to innovate	Scalability, flexibility and agility, Ease of use
Leverage new HR tools and services to onboard and manage talent	Bigger knowledge market
Moving technology upstream as a driver of strategy and business models	Governmental strategy
Opportunity to address the exponential growth in technology systems and data	Improved hard- and software, Improved integration and interoperability
Provide and enhance data-driven insights	Improved integration and interoperability internally and externally
Support new business models at scale, operationally	Scalability, flexibility and agility
The rapid pace of technology change and the ability to keep up	Scalability, flexibility and agility & Improved hard- and software
Attracting and retaining new cloud hires	Bigger knowledge market
Organisation’s ability to embrace change	Scalability, flexibility and agility

TABLE C.1: Cross-reference drivers with company documents

Source: BIO	Goal	Risk	Barrier
B.01 Law and regulation cloud services	To prevent the violation of laws, or any contractual or regulatory demands and security demands, by explicitly determining the relevant requirements and keeping them up to date	Damage due to legal liability (as a consequence of outdated, undocumented or unclear requirements)	Regulations and government policy
B.02 Cloudsecurity strategy	Clear cloud security strategy, that is coherent with the strategic goals of the CSP and that supports information secuity demonstrable.	The lack of an agreed guideline/global approach to securing cloud services.	Regulations and government policy
B.03 Exit strategy cloud services	Exit strategy needs to be determined before the CSC and CSP enter their "collaboration" in this strategy, terms and conditions under which the CSC can end the contract will be present. This is to improve interoperability, to mitigate the risk of a vendor lock-in. (often Exit strategy is present in SLA)	The lack of an agreed guideline/global approach to the termination of Cloud service Provider contracts	Fear of losing control
B.04 Cloud service policy	The CSP needs to make the cloud service security part of its information security strategy, which includes access procedures, the cycle of accounts etc. to ensure that the CSC gets products with which it can achieve its goals	Lack of control over the cloud services, which causes an inability to not fulfil their intended use.	Lack of knowledge
B.05 Transparency	To give insight in the implementation and functioning of the cloud services, a systemdescription is provided where jurisdiction, research posibilities and certificates are adressed.	The CSP proves a services that is not fully tailored to the needs of the CSC	Fear of losing control
B.06 Risk management	The CSP needs to create and maintain the (shared) responsibility and risk management process.	The measures are under-, or overprotecting the cloud services	Data security concerns
B.07 IT functionality	To ensure that the IT functionality is according the necessary safety measures, the IT functionality need to be provided from a robust and secure systemchain from CSP to CSC.	The IT functionality is a weak link in the security	Data security concerns
B.08 Business continuity management	To be able to to resume business within a critical time period in case of system failure, the CSP develops a Business Continuity Management (BCM)-process.	Inadequately reacting to failure, resulting in more damage than necessary	Lack of standards
B.09 Privacy and protection personal data	To ensure privacy measures are being complied with, the CSP needs to show that data is protected in all stages, show who has acces and ownership, show the ownership of the data and the location	Data is under secured	Data security concerns
B.10 Security organisation	The CSP needs to have a security function (organisational department) that supports the information security within the CSP.	Cloud service policy is not accurately enforced	Data security concerns
B.11 Cloud service architecture	The CSP should document the current architecture and provide a cloud service landscape where the (in)dependencies of the IT functionalities are depicted, to guarantee the reliable working of the cloud services.	No or limited control over cloud services. Cloud services are unreliable.	Legacy dependence

U.01 Standards for cloud services	To obtain the necessary coordination of activities necessary for the design, operation and control of cloud services. National and international standards should be demonstrably applied by the CSP.	Generic risks are not mitigated	Lack of standards
U.02 Risk assessment	To define possible risks, the CSP needs to perform a risk assessment (e.g. for threats and vulnerabilities).	No or limited insight on the risks related to cloud services	Lack of knowledge
U.03 Business continuity services	To make sure that during failure, information processes are back on track within in the maximum down time limit to decrease data loss and to meet the continuity demands.	Systems are down longer than the specified time	Fear of losing control
U.04 Recovery of data an services	DR needs to be tested periodically and robustly to ensure system and data recovery	To pass the limit of maximum data loss/down time	Fear of losing control
U.05 Data protection	Data that is classified BBN2 or higher, should be secured in compliance with Dutch law	Data classified as BBN2 or higher is not sufficiently protected	Data security concerns
U.06 Data retention and destruction	Data should be available within the specified window for (destruction) requests for the CSC and during this window securely stored.	The integrity of the data is affected and/or it is stored longer than the agreed timeframe	Data security concerns
U.07 Data separation	The CSC's control functions and data should be isolated from other customers of the same CSP during transport, processing and storage.	Other CSCs and the CSP get access to the data or control of the CSP and vice versa.	Data security concerns
U.08 Service separation	The cloud infrastructure should be designed such that the CSCs are isolated from each other, and also the CSP's internal communication should be separated from the CSC's services.	Data alteration or communication or data	Fear of losing control
U.08 Service separation	The cloud infrastructure should be designed such that the CSPs are isolated from each other, and also the CSP's internal communication should be separated from the CSC's services.	Data alteration or communication or data	Fear of losing control
U.09 Malware protection	To protect against malware, measures for detection, prevention and recovery in combination with a conscious attitude by their users are of vital importance.	Malware is detected not or too late, and can not or only in limited amount be recovered	Data security concerns
U.10 Access IT services and data	Users can only access IT services that they are authorised to access.	Abuse and loss of (sensitive data) due to unauthorised access.	Data security concerns
U.11 Crypto sevices	To protect sensitive data during network transit and storage, it should be encrypted according to current regulations.	Data is accessible to unauthorised persons in transit and storage.	Data security concerns

U.12 Interfaces	To prevent data leaks, the interfaces between the CSC and the CSP should be guarded and limited.	Data of the CSC is transferred to the CSP through one of the interfaces.	Data security concerns
U.13 Service orchestration	The actual services are in compliance with the previously established QoS, information security and costs. The service orchestration provides coordination and aggregation of the cloud service components.	No or insufficient coordination, aggregation or composition of service components	Fear of losing control
U.14 Interoperability and portability	The cloud services are usable on different IT platforms (due to standards) and can connect different platforms with each other (Interoperability). Data can be transferred to different CSPs without major modifications (Portability).	Lack of portability and interoperability	Lack of standards
U.15 Logging and monitoring	Log files with (irregular) usage data and information security data should be stored and regularly monitored to detect strange activity.	Irregularities can not be investigated, and recovery can not be done, due to the absence of log files.	Fear of losing control
U.16 Cloud service architecture	In the cloud service architecture, the CSP specifies the functional relationship between the IT-components of the CSC and the CSP. This should provide transparency and provides an overview of the boundary conditions and the set-up in general, as well as the supply and portability of the data.	The functional relationship is not well defined, which results in risks related to data control	Fear of losing control
U.17 Multi-tenant architecture	The CSC data that is used within cloud services that are also used by other CSCs (multi-tenancy), is encrypted in rest and processed in isolation on separate (virtual) machines.	Multi-tenancy brings additional risks.	Data security concerns
C.01 Servicemanagement policy and evaluation guideline	The CSP has a servicemanagement policy with defined guidelines for governance processes, control activities and reports.	The results of the control activities that are executed on cloud services do not fulfil the requirements	Fear of losing control
C.02 Risk-control	The continuous process of monitoring and reviewing the risk-assessment process to detect changes that alter the results of the assessment	Anticipate too late (or not at all) to risk factors that influence the assessment	Internal resistance to change
C.03 Compliance and assurance	The CSP reviews the adherence to the cloud security agreement on compliancy and compares this review to the results of an assurance report. These results are presented to the CSC.	Having no control or certainty on compliance to current rules and regulations, or the security level in general.	Fear of losing control
C.04 Technical vulnerabilities	Collecting and controlling security vulnerabilities (by the CSP) and communicating them transparently to the CSC. Exposure to vulnerabilities should be accompanied by an evaluation and suiting measures to deal with possible damage to the CSC.	Technical vulnerabilities are not (too late) discovered	Data security concerns

C.05 Security and monitoring	The performance of the information security of the cloud environment should be monitored and reported to relevant stakeholders, to maintain a chain of evidence.	Abuse of performance of information security of cloud environment.	Data security concerns
C.06 Management organisation	CSP has a management organisation in which the process structure, tasks, responsibilities and authorisation of the relevant roles/people/functions are stated.	The cloud services are not following necessary steps.	Lack of standards

Appendix D

SSIM

Barriers

	BR1	BR2	BR3	BR4	BR5	BR6	BR7	BR8
BR1		10, 1, 11, 0	10, 3, 2, 7	7, 3, 1, 11	12, 1, 5, 4	9, 4, 2, 7	6, 6, 9, 1	12, 2, 0, 8
BR2			7, 2, 12, 1	3, 10, 4, 5	4, 10, 6, 2	1, 15, 5, 1	2, 7, 11, 2	15, 1, 0, 6
BR3				2, 14, 3, 3	2, 13, 3, 4	1, 13, 8, 0	1, 15, 5, 1	4, 8, 5, 5
BR4					6, 5, 2, 9	5, 10, 5, 2	8, 3, 1, 10	18, 1, 1, 2
BR5						3, 6, 9, 4	17, 0, 2, 3	14, 2, 1, 5
BR6							18, 0, 4, 0	17, 0, 3, 2
BR7								11, 2, 2, 7
BR8								

TABLE D.1: Aggregated structural self interaction matrix. Frequency of recognised contextual relationship in order V, A, X, O.

Drivers

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8
DR1		14, 0, 6, 2	1, 17, 1, 3	2, 12, 7, 1	2, 13, 5, 2	2, 15, 4, 1	2, 16, 4, 0	2, 12, 6, 2
DR2			4, 8, 1, 9	6, 6, 5, 5	3, 12, 5, 2	5, 7, 2, 8	6, 7, 4, 5	6, 9, 6, 1
DR3				5, 3, 8, 6	4, 6, 3, 9	8, 6, 3, 5	5, 9, 4, 4	5, 12, 3, 2
DR4					8, 9, 3, 2	13, 0, 6, 3	12, 3, 4, 3	3, 5, 11, 3
DR5						14, 1, 1, 6	12, 5, 1, 4	2, 7, 5, 8
DR6							8, 6, 2, 6	4, 12, 2, 4
DR7								1, 10, 6, 5
DR8								

TABLE D.2: Aggregated structural self-interaction matrix for drivers. Frequency of recognised contextual relationship in order V, A, X, O.

Appendix E

Results RM for different thresholds

	BR1	**BR2**	**BR3**	**BR4**	**BR5**	**BR6**	**BR7**	**BR8**
BR1	1	1	0	0	1	0	1	0
BR2	0	1	1	0	0	0	0	1
BR3	0	0	1	0	0	0	0	0
BR4	0	0	1	1	0	0	0	1
BR5	0	1	1	0	1	0	1	1
BR6	0	1	1	1	1	1	1	1
BR7	1	1	1	0	0	0	1	0
BR8	0	0	0	0	0	0	0	1

TABLE E.1: The final binary direct reachability matrix using a threshold of 14

	BR1	**BR2**	**BR3**	**BR4**	**BR5**	**BR6**	**BR7**	**BR8**
BR1	1	1	0	0	1	0	0	0
BR2	0	1	1	0	0	0	0	0
BR3	0	0	1	0	0	0	0	0
BR4	0	0	1	1	0	0	0	1
BR5	0	0	0	0	1	0	1	0
BR6	0	1	1	0	0	1	1	1
BR7	0	1	1	0	0	0	1	0
BR8	0	0	0	0	0	0	0	1

TABLE E.2: The final binary direct reachability matrix using a threshold of 16

	DR1	**DR2**	**DR3**	**DR4**	**DR5**	**DR6**	**DR7**	**DR8**
DR1	1	1	0	0	0	0	0	0
DR2	0	1	0	0	0	0	0	0
DR3	1	1	1	0	0	0	0	0
DR4	0	0	0	1	0	1	1	0
DR5	1	0	1	0	1	1	1	0
DR6	1	1	0	0	0	1	0	0
DR7	1	0	0	0	0	0	1	0
DR8	0	0	0	0	1	1	1	1

TABLE E.3: The final binary direct reachability matrix using a threshold of 14 for the drivers

	DR1	**DR2**	**DR3**	**DR4**	**DR5**	**DR6**	**DR7**	**DR8**
DR1	1	0	0	0	0	0	0	0
DR2	0	1	0	0	0	0	0	0
DR3	1	1	1	0	0	0	0	0
DR4	0	0	0	1	0	0	0	0
DR5	0	0	0	0	1	1	0	0
DR6	0	0	0	0	0	1	0	0
DR7	0	0	0	0	0	0	1	0
DR8	0	0	0	0	0	0	0	1

TABLE E.4: The final binary direct reachability matrix using a threshold of 16 for the drivers

Appendix F

Graphs with transitive links

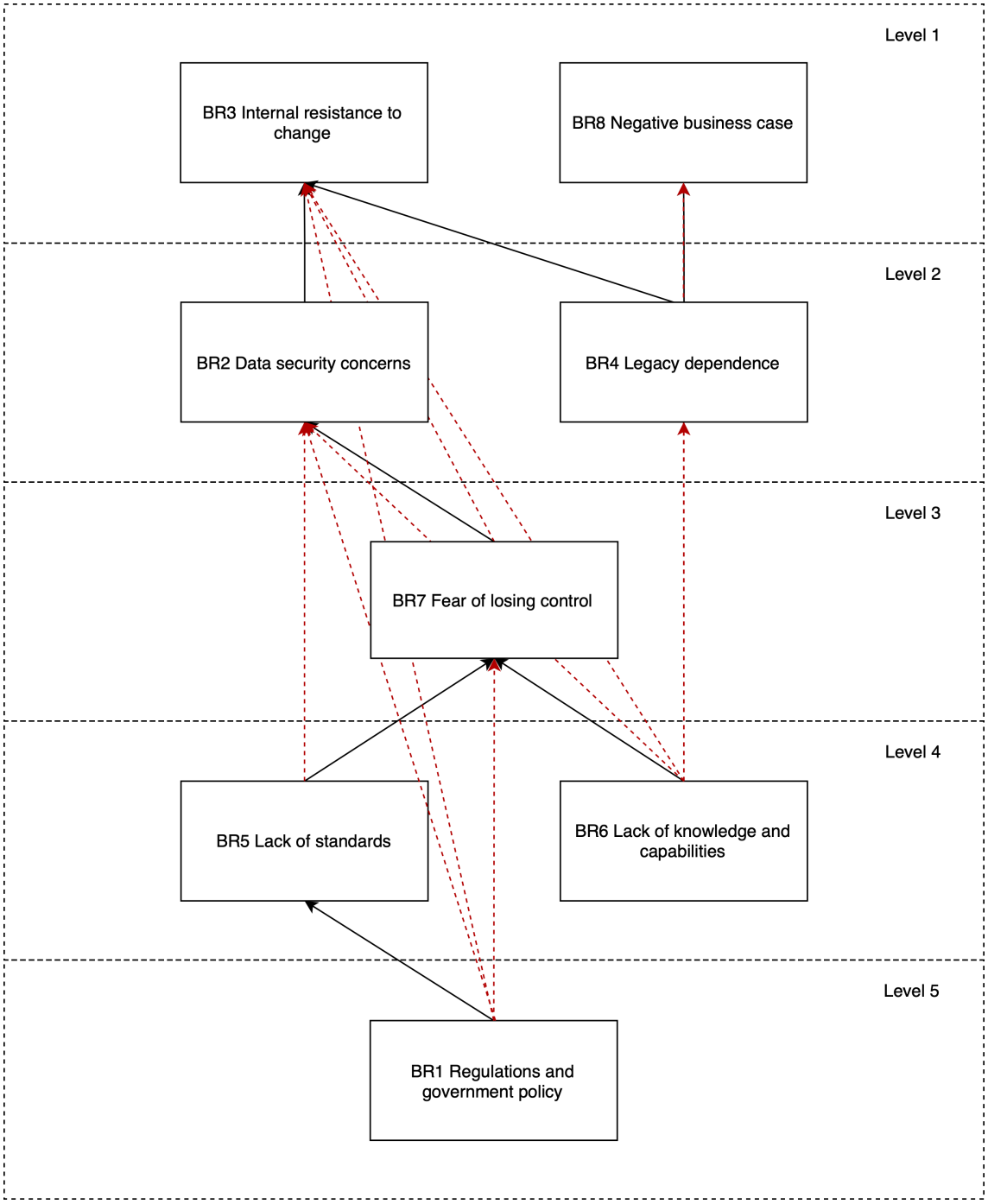

FIGURE F.1: Final directed graph barriers including transitive links

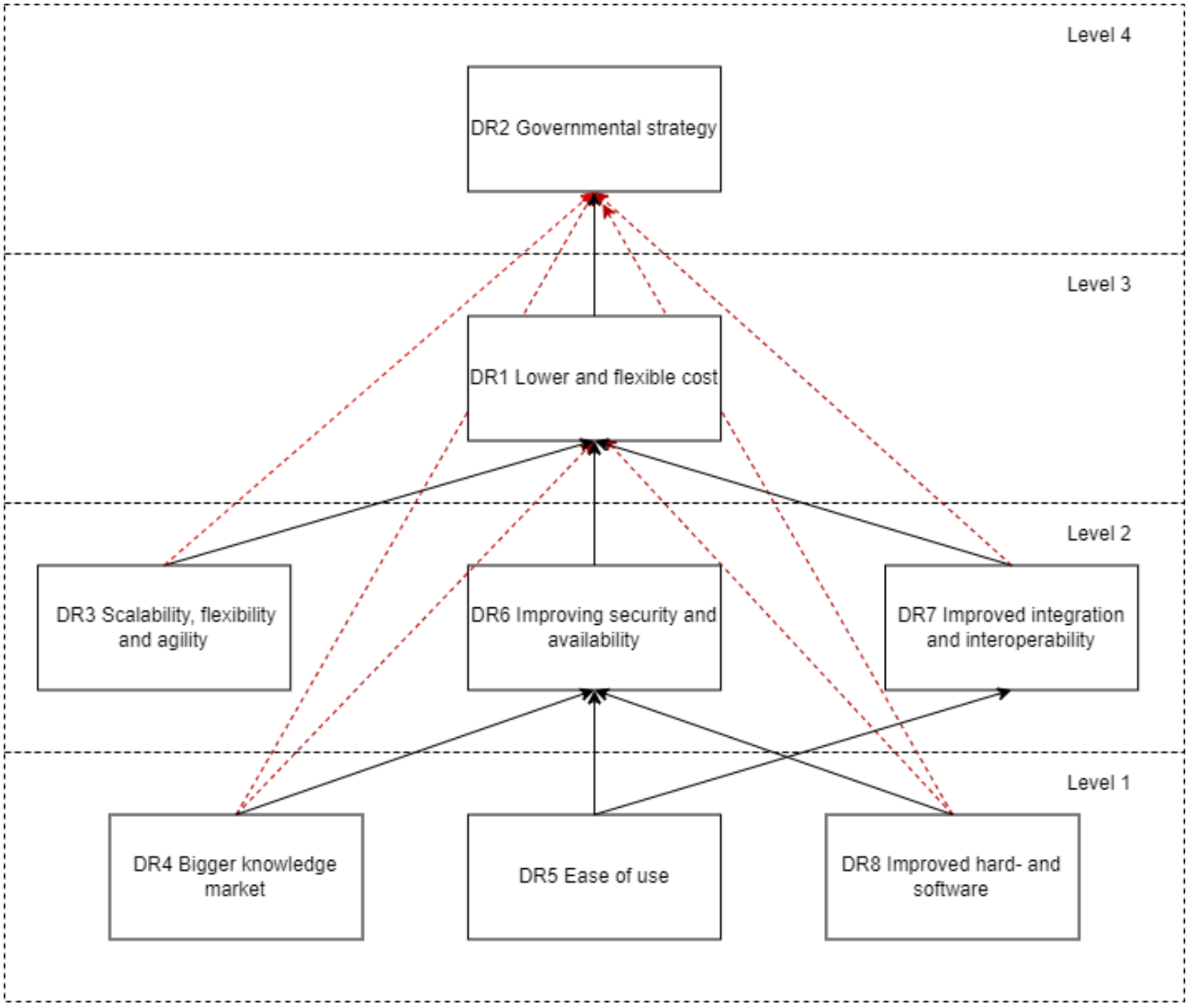

FIGURE F.2: Final directed graph drivers including transitive links

Appendix G

Results fuzzy MICMAC for different parameters

The aggregated matrix that is determined by taking the average of all individual fuzzy direct reachability matrices is presented in table G.3. After averaging the entries, the matrix is normalised by taking the largest entry in the matrix (i.e. 0.84) and the smallest (i.e. 0.05) and replacing the elements according to: x_{ij} is replaced by $x_{ij} - min_{entry}/(max_{entry} - min_{entry})$. For the normalised results, both drivers and barriers stabilised after 7 iterations. The resulting dependence-driver graphs are shown in G.1 and G.2.

	BR1	BR2	BR3	BR4	BR5	BR6	BR7	BR8	Driving	Level
BR1	0,5	0,5	0,5	0,4	0,5	0,4	0,5	0,5	3,8	1
BR2	0,5	0,5	0,5	0,4	0,5	0,4	0,5	0,5	3,8	1
BR3	0,5	0,5	0,5	0,4	0,5	0,4	0,5	0,5	3,8	1
BR4	0,5	0,5	0,5	0,4	0,5	0,4	0,5	0,5	3,8	1
BR5	0,5	0,5	0,5	0,4	0,5	0,4	0,5	0,5	3,8	1
BR6	0,5	0,5	0,5	0,4	0,5	0,4	0,5	0,5	3,8	1
BR7	0,5	0,5	0,5	0,4	0,5	0,4	0,5	0,5	3,8	1
BR8	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	3,2	2
Dependence	3,9	3,9	3,9	3,2	3,9	3,2	3,9	3,9		
Level	1	1	1	2	1	2	1	1		

TABLE G.1: Stabilized fuzzy matrix barriers 1 decimal

	BR1	BR2	BR3	BR4	BR5	BR6	BR7	BR8	Driving	Level
BR1	0,5	0,5	0,5	0,35	0,5	0,35	0,5	0,45	3,65	1
BR2	0,45	0,45	0,5	0,35	0,45	0,35	0,45	0,45	3,45	2
BR3	0,45	0,5	0,45	0,35	0,45	0,35	0,45	0,45	3,45	2
BR4	0,45	0,45	0,5	0,35	0,45	0,35	0,45	0,45	3,45	2
BR5	0,5	0,5	0,5	0,35	0,5	0,35	0,5	0,45	3,65	1
BR6	0,5	0,5	0,5	0,35	0,5	0,35	0,5	0,45	3,65	1
BR7	0,5	0,5	0,5	0,35	0,5	0,35	0,5	0,45	3,65	1
BR8	0,38	0,38	0,38	0,35	0,38	0,35	0,38	0,38	2,98	3
Dependence	3,73	3,78	3,83	2,8	3,73	2,8	3,73	3,53		
Level	3	2	1	5	3	5	3	4		

TABLE G.2: Stabilized fuzzy matrix barriers 2 decimal

	BR1	BR2	BR3	BR4	BR5	BR6	BR7	BR8
BR1	0	0,78	0,36	0,26	0,57	0,23	0,51	0,31
BR2	0,44	0	0,67	0,22	0,4	0,23	0,45	0,44
BR3	0,16	0,5	0	0,17	0,13	0,35	0,23	0,24
BR4	0,15	0,43	0,61	0	0,24	0,33	0,24	0,72
BR5	0,24	0,57	0,36	0,23	0	0,34	0,56	0,38
BR6	0,19	0,77	0,82	0,49	0,44	0	0,84	0,64
BR7	0,5	0,64	0,73	0,13	0,07	0,14	0	0,45
BR8	0,08	0,05	0,38	0,08	0,09	0,1	0,13	0

TABLE G.3: Aggregated average fuzzy direct reachability matrix barriers

	BR1	BR2	BR3	BR4	BR5	BR6	BR7	BR8
BR1	0	0,92	0,39	0,27	0,66	0,23	0,58	0,33
BR2	0,49	0	0,78	0,22	0,44	0,23	0,51	0,49
BR3	0,14	0,57	0	0,15	0,1	0,38	0,23	0,24
BR4	0,13	0,48	0,71	0	0,24	0,35	0,24	0,85
BR5	0,24	0,66	0,39	0,23	0	0,37	0,65	0,42
BR6	0,18	0,91	0,97	0,56	0,49	0	1	0,75
BR7	0,57	0,75	0,86	0,1	0,03	0,11	0	0,51
BR8	0,04	0	0,42	0,04	0,05	0,06	0,1	0

TABLE G.4: Normalized fuzzy matrix barriers

	BR1	BR2	BR3	BR4	BR5	BR6	BR7	BR8	Driving	Level
BR1	0,57	0,57	0,57	0,38	0,57	0,38	0,57	0,51	4,12	1
BR2	0,51	0,51	0,57	0,38	0,51	0,38	0,51	0,51	3,88	2
BR3	0,51	0,57	0,51	0,38	0,51	0,38	0,51	0,51	3,88	2
BR4	0,51	0,51	0,57	0,38	0,51	0,38	0,51	0,51	3,88	2
BR5	0,57	0,57	0,57	0,38	0,57	0,38	0,57	0,51	4,12	1
BR6	0,57	0,57	0,57	0,38	0,57	0,38	0,57	0,51	4,12	1
BR7	0,57	0,57	0,57	0,38	0,57	0,38	0,57	0,51	4,12	1
BR8	0,42	0,42	0,42	0,38	0,42	0,38	0,42	0,42	3,28	3
Dependence	4,23	4,29	4,35	3,04	4,23	3,04	4,23	3,99		
Level	3	2	1	5	3	5	3	4		

TABLE G.5: Stabilized fuzzy normalized matrix barriers

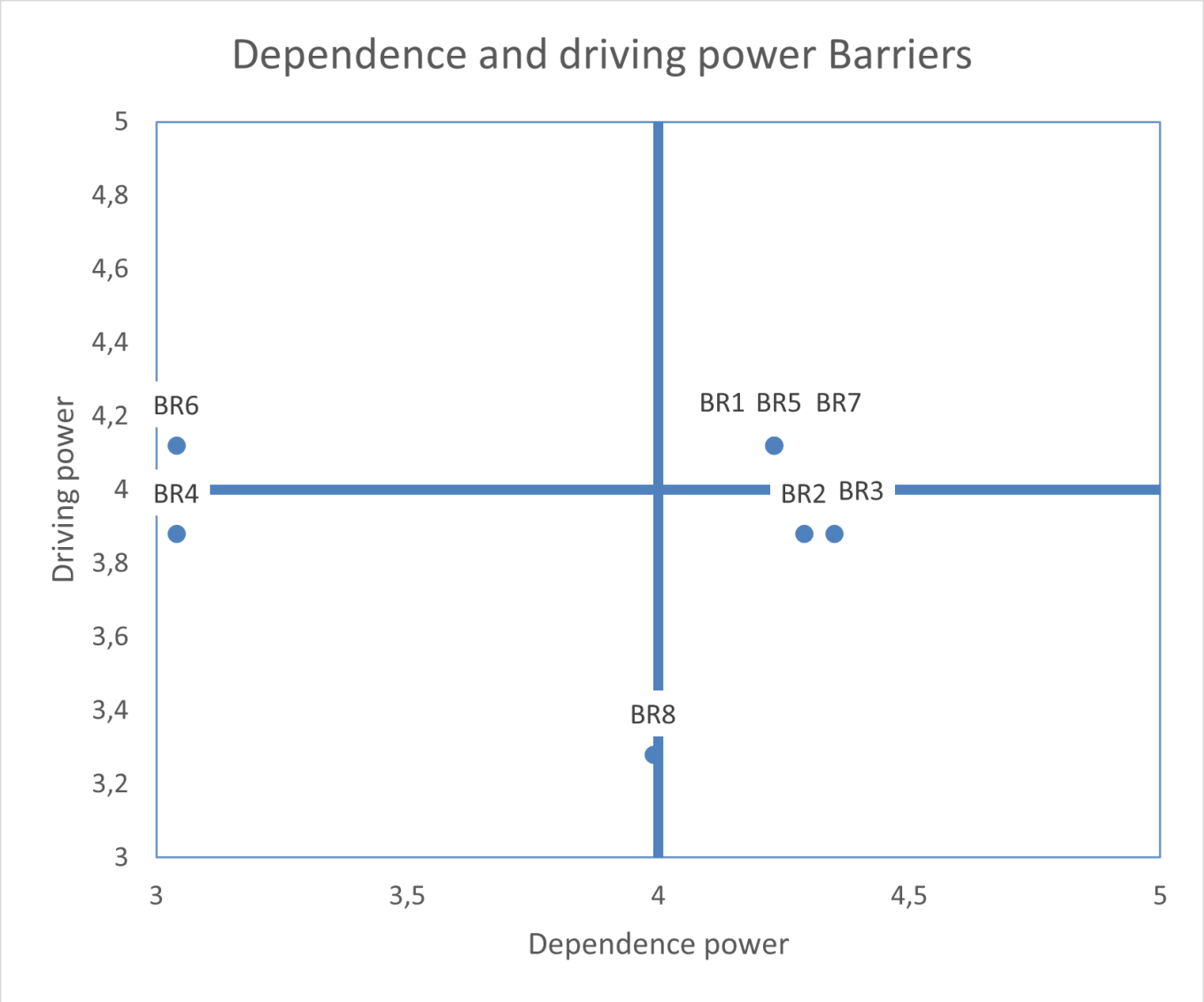

FIGURE G.1: Driving and dependence power of barriers normalized fuzzy matrix

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8	Driver	Level
DR1	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,3	3,1	4
DR2	0,4	0,4	0,4	0,4	0,4	0,5	0,4	0,3	3,2	3
DR3	0,5	0,5	0,4	0,4	0,4	0,4	0,4	0,3	3,3	2
DR4	0,4	0,4	0,4	0,4	0,4	0,5	0,4	0,3	3,2	3
DR5	0,4	0,4	0,4	0,4	0,4	0,5	0,4	0,3	3,2	3
DR6	0,5	0,5	0,4	0,4	0,4	0,4	0,4	0,3	3,3	2
DR7	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,3	3,1	4
DR8	0,5	0,5	0,4	0,4	0,4	0,5	0,4	0,3	3,4	1
Dependence	3,5	3,5	3,2	3,2	3,2	3,6	3,2	2,4		
Level	2	2	3	3	3	1	3	4		

TABLE G.6: Stabilized fuzzy matrix drivers 1 decimal

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8	Driver	Level
DR1	0,44	0,44	0,44	0,36	0,43	0,44	0,43	0,33	3,31	4
DR2	0,44	0,44	0,44	0,36	0,43	0,48	0,43	0,33	3,35	3
DR3	0,48	0,48	0,44	0,36	0,43	0,44	0,43	0,33	3,39	2
DR4	0,44	0,44	0,44	0,36	0,43	0,48	0,43	0,33	3,35	3
DR5	0,44	0,44	0,44	0,36	0,43	0,48	0,43	0,33	3,35	3
DR6	0,48	0,48	0,44	0,36	0,43	0,44	0,43	0,33	3,39	2
DR7	0,44	0,44	0,44	0,36	0,43	0,44	0,43	0,33	3,31	4
DR8	0,48	0,48	0,44	0,36	0,43	0,48	0,43	0,33	3,43	1
Dependence	3,64	3,64	3,52	2,88	3,44	3,68	3,44	2,64		
Level	2	2	3	5	4	1	4	6		

TABLE G.7: Fuzzy stabilized matrix drivers 2 decimals

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8
DR1	0,00	0,44	0,13	0,05	0,15	0,11	0,06	0,15
DR2	0,06	0,00	0,44	0,34	0,11	0,48	0,38	0,13
DR3	0,76	0,53	0,00	0,32	0,43	0,44	0,28	0,16
DR4	0,30	0,31	0,24	0,00	0,31	0,50	0,42	0,13
DR5	0,45	0,40	0,49	0,36	0,00	0,72	0,52	0,33
DR6	0,52	0,55	0,34	0,10	0,23	0,00	0,42	0,28
DR7	0,48	0,33	0,41	0,19	0,32	0,32	0,00	0,17
DR8	0,50	0,30	0,45	0,18	0,55	0,58	0,41	0,00

TABLE G.8: Aggregated average fuzzy direct reachability matrix drivers

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8
DR1	0	0,55	0,11	0	0,14	0,08	0,01	0,14
DR2	0,01	0	0,55	0,41	0,08	0,61	0,46	0,11
DR3	1	0,68	0	0,38	0,54	0,55	0,32	0,15
DR4	0,35	0,37	0,27	0	0,37	0,63	0,52	0,11
DR5	0,56	0,49	0,62	0,44	0	0,94	0,66	0,39
DR6	0,66	0,7	0,41	0,07	0,25	0	0,52	0,32
DR7	0,61	0,39	0,51	0,2	0,38	0,38	0	0,17
DR8	0,63	0,35	0,56	0,18	0,7	0,75	0,51	0

TABLE G.9: Normalized fuzzy matrix drivers

	DR1	DR2	DR3	DR4	DR5	DR6	DR7	DR8	Driver	Level
DR1	0,55	0,55	0,55	0,44	0,54	0,55	0,54	0,39	4,11	4
DR2	0,55	0,55	0,55	0,44	0,54	0,61	0,54	0,39	4,17	3
DR3	0,61	0,61	0,55	0,44	0,54	0,55	0,54	0,39	4,23	2
DR4	0,55	0,55	0,55	0,44	0,54	0,61	0,54	0,39	4,17	3
DR5	0,55	0,55	0,55	0,44	0,54	0,61	0,54	0,39	4,17	3
DR6	0,61	0,61	0,55	0,44	0,54	0,55	0,54	0,39	4,23	2
DR7	0,55	0,55	0,55	0,44	0,54	0,55	0,54	0,39	4,11	4
DR8	0,61	0,61	0,55	0,44	0,54	0,61	0,54	0,39	4,29	1
Dependence	4,58	4,58	4,4	3,52	4,32	4,64	4,32	3,12		
Level	2	2	3	5	4	1	4	6		

TABLE G.10: Stabilized fuzzy normalized matrix drivers

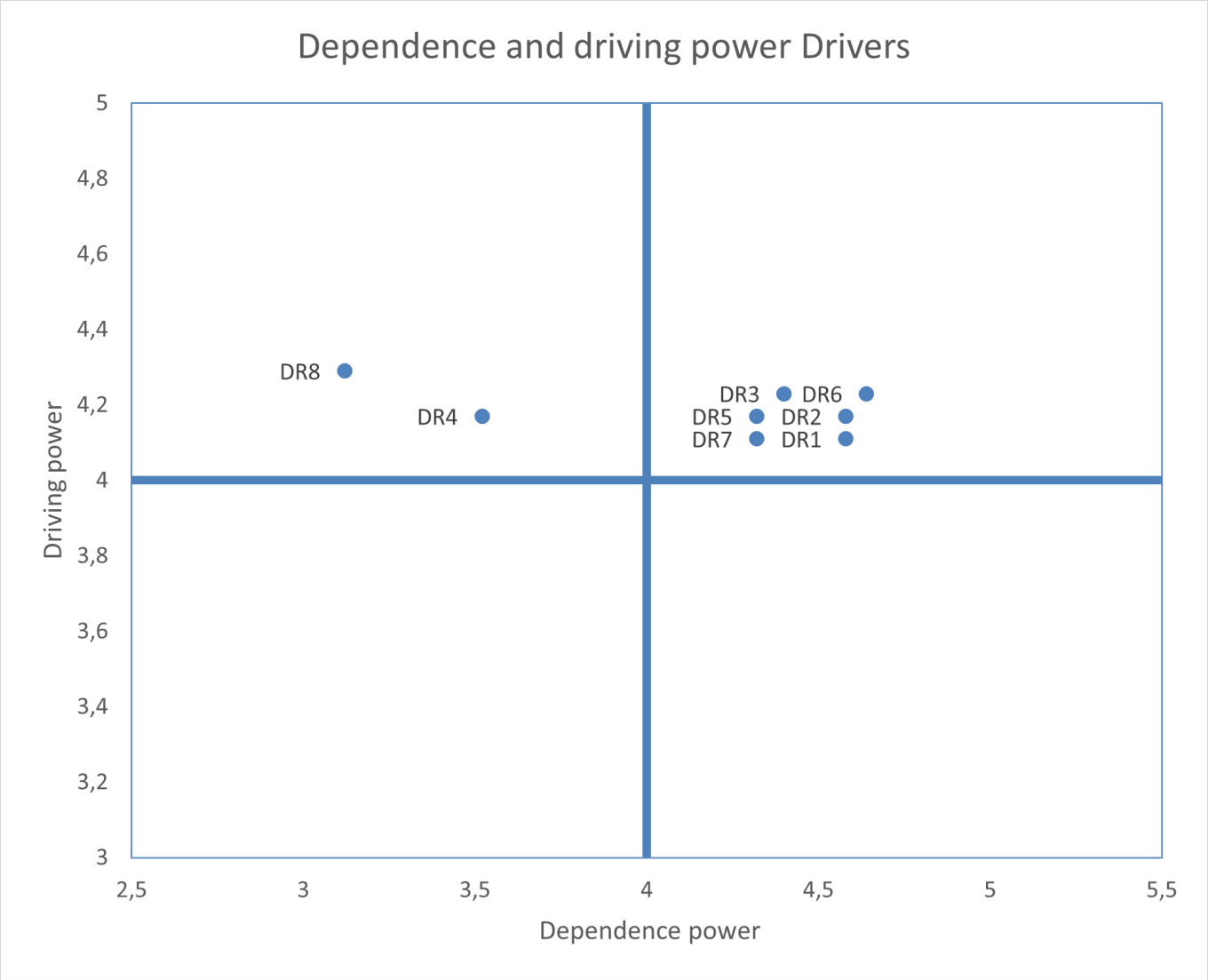

FIGURE G.2: Driving and dependence power of drivers

Appendix H

Interview slides

In this appendix, the interview slides that were used during the expert interviews to develop the pairwise contextual relationship between factors are presented. The slides are in Dutch since all the interviewees were native Dutch speakers and this would limit the communication barrier.

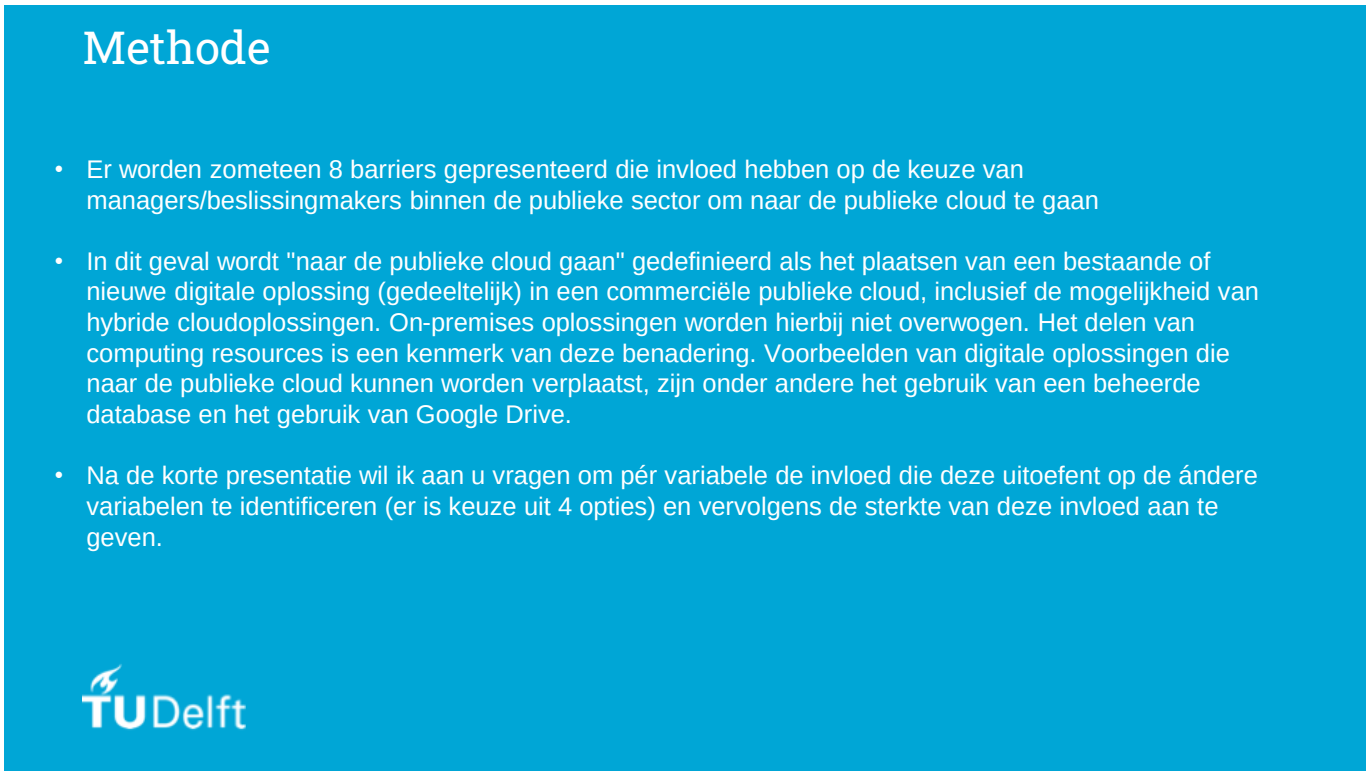

FIGURE H.1: Interview slide 1

Barrier	Description
Regulations and government policy	Absence of legal frameworks, as well as a uniform and easy to use governmental cloud protocol.
Data security concerns	Vulnerable to attacks, due to bigger attack surface. Data integrity and confidentiality.
Internal resistance to change	Unwillingness to adapt to new circumstances.
Legacy dependence	There is a lack of compatibility, switching costs.
Lack of standards	There is a lack of standards internally (legacy) and a lack of standards externally (strategic direction government) (no guarantee of data portability).
Lack of knowledge and capabilities	The lack of IT-skilled personnel within the governmental authorities. Difficult to assess possibilities. Shift from application management to functional management.
Losing control	Fear of losing digital sovereignty of data. Assurance and compliance issues. Fear of a vendor lock-in.
Negative business case	Insufficient substantiation for choice to use public cloud technology. “Need to use” public cloud insufficient.

TUDelft

FIGURE H.2: Interview slide 2

Q1: What is the relation between variable A and the variables in column B:

- A influences B
- B influences A
- A and B influence each other
- A and B are unrelated

Q2: How strong is this relation:

- Very weak
- Weak
- Strong
- Very strong

TUDelft

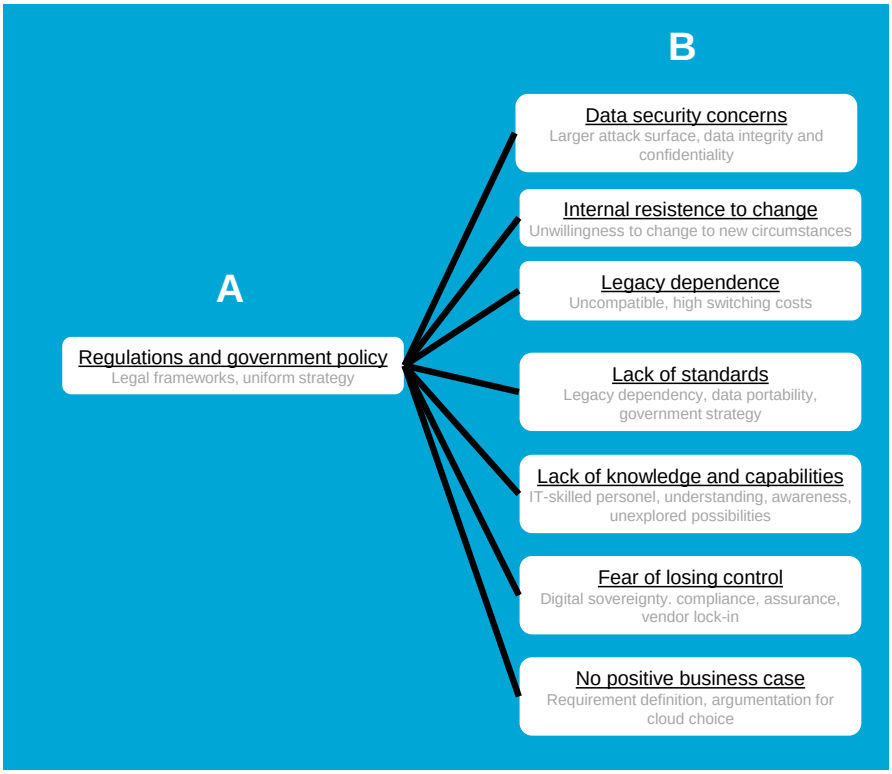

FIGURE H.3: Interview slide 3

Appendix I

Informed consent

The informed consent was sent to the participants. It was written in Dutch since all the interviewees were native Dutch speakers and this would limit the communication barrier.

Research Informed Consent

U wordt uitgenodigd om deel te nemen aan een onderzoek genaamd "factoren die cloud adoptie beinvloeden in de Nederlandse publieke sector" Dit onderzoek wordt uitgevoerd door Marleen van Merrienboer van de TU Delft, tijdens een stage bij Deloitte.

Het doel van dit onderzoek is het analyseren en visualiseren van onderlinge relaties tussen factoren die invloed hebben op de keuze om publieke cloud te adopteren in de publieke sector en zal ongeveer 2x60 minuten in beslag nemen. De data zal gebruikt worden voor een masterscriptie met mogelijke publicatie, en om beslissingen en beleidsmakers binnen de publieke sector te ondersteunen. U wordt gevraagd om aan te geven in hoeverre een gepresenteerde factor *i* invloed heeft op factor *j*. Dit process herhaalt zich voor 16 factoren.

Zoals bij elke online activiteit is het risico van een databreuk aanwezig. Wij doen ons best om uw antwoorden vertrouwelijk te houden. We minimaliseren de risico's door data anoniem te verzamelen en in een beveiligde survey database op te slaan. De informatie die wordt opgeslagen is:

-De antwoorden op de survey
-De functienaam van de geïnterviewde (e.g. manager IT-afdeling, developer etc.)
-Het aantal jaren werkervaring
-Het gegeven dat de geïnterviewde werkzaam is in de publieke sector

Uw deelname aan dit onderzoek is volledig vrijwillig, en u kunt zich elk moment terugtrekken zonder reden op te geven. U bent vrij om vragen niet te beantwoorden.

PLEASE TICK THE APPROPRIATE BOXES	Yes	No
A: GENERAL AGREEMENT – RESEARCH GOALS, PARTICPANT TASKS AND VOLUNTARY PARTICIPATION		
1. Ik heb de informatie over het onderzoek gelezen en begrepen, of deze is aan mij voorgelezen. Ik heb de mogelijkheid gehad om vragen te stellen over het onderzoek en mijn vragen zijn naar tevredenheid beantwoord.	☐	☐
2. Ik doe vrijwillig mee aan dit onderzoek, en ik begrijp dat ik kan weigeren vragen te beantwoorden en mij op elk moment kan terugtrekken uit de studie, zonder een reden op te hoeven geven.	☐	☐
3. Ik begrijp dat mijn deelname aan het onderzoek de volgende punten betekent:	☐	☐
• *De informatie wordt door vastgelegd middel van een begeleide vragenlijst* • *De informatie wordt verzameld door middel van handgeschreven notities* • *De informatie wordt opgeslagen in een beveiligde surveydatabase*		
5. Ik begrijp dat de studie 14-08-2023 eindigt.		
B: POTENTIAL RISKS OF PARTICIPATING (INCLUDING DATA PROTECTION)		
6. Ik begrijp dat mijn deelname de volgende risico's met zich meebrengt […]. Ik begrijp dat deze risico's worden geminimaliseerd door […]	☐	☐
• *Anonieme data verwerking* • *Beveiligde vragenlijst datanbase*		

PLEASE TICK THE APPROPRIATE BOXES	Yes	No
10. Ik begrijp dat de persoonlijke informatie die over mij verzameld wordt en mij kan identificeren, zoals naam en wekplaats, niet gedeeld worden buiten het studieteam.	☐	☐
11. Ik begrijp dat de persoonlijke data die over mij verzameld wordt, vernietigd wordt binnen 4 maanden na het interview	☐	☐
C: RESEARCH PUBLICATION, DISSEMINATION AND APPLICATION		
12. Ik begrijp dat na het onderzoek de geanonimiseerde informatie gebruikt zal worden voor […]	☐	☐
• *Master scriptie rapport* • *Mogelijke publicatie* • *Beslissings ontwikkeling* • *Beleidsontwikkeling*		
D: (LONGTERM) DATA STORAGE, ACCESS AND REUSE		
16. Ik geef toestemming om de geanonimiseerde data [*Zie onderstaande lijst*] die over mij verzameld worden gearchiveerd worden in de TU Delft Thesis repository opdat deze gebruikt kunnen worden voor toekomstig onderzoek en onderwijs.	☐	☐
• *De antwoorden op de survey* • *De functienaam van de geïnterviewde (e.g. manager IT-afdeling, developer etc.)* • *Het aantal jaren werkervaring* • *Het gegeven dat de geïnterviewde werkzaam is in de publieke sector*		

Signatures

_____	_____	_____
Naam deelnemer	Handtekening	Datum

Ik, **de onderzoeker**, verklaar dat ik de informatie en het instemmingsformulier correct aan de potentiële deelnemer heb verstuurd en naar het beste van mijn vermogen, heb verzekerd dat de deelnemer begrijpt waar hij/zij vrijwillig mee instemt.

Marleen van Merrienboer	_____	12-06-2023
Naam onderzoeker	Handtekening	Datum