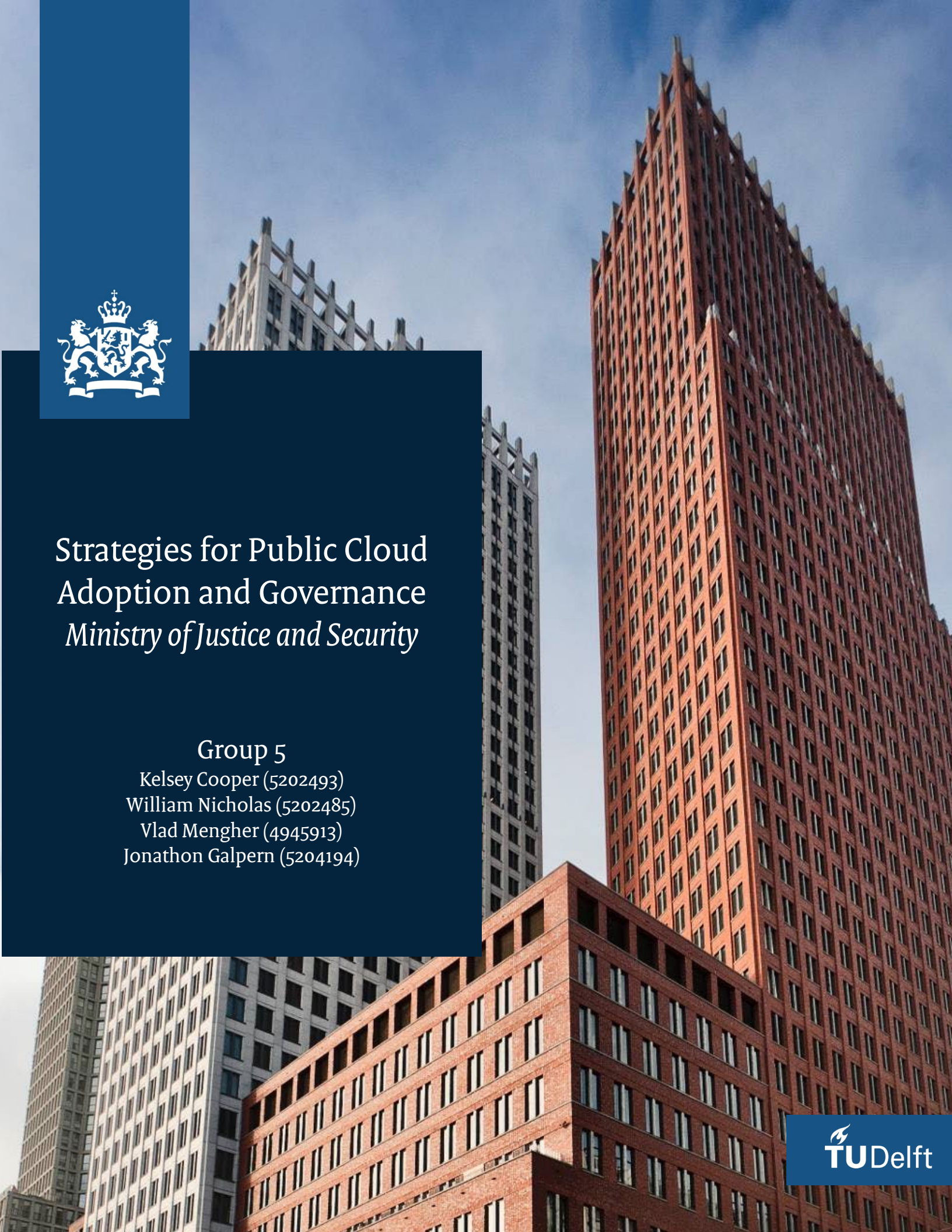


Strategies for Public Cloud Adoption and Governance

Ministry of Justice and Security

Group 5

Kelsey Cooper (5202493)
William Nicholas (5202485)
Vlad Mengher (4945913)
Jonathon Galpern (5204194)

TU Delft

Executive Summary

The European Commission reports that enterprises in the Netherlands utilize cloud computing at a rate of 48%, making the country the one of Europe's most cloud-savvy nations. This rise of cloud computing adoption in the private sector parallels growth around the world and signals a change in the way technology is stored and managed. As the use of public cloud technology expands to include many of the key software packages on which organizations rely, it is important the Ministry of Justice and Security remain well-equipped to accomplish its mission. It is therefore necessary that the Ministry move carefully but decisively to ensure a successful adoption of public cloud.

In this report, we evaluate the structure of the Ministry of Justice and Security, its key stakeholders, and the problem of adopting and governing public cloud technology. We then consider the risks inherent in the implementation process, as well as the decision-making arena, including critical governance actors. Later, we present potential solutions and weigh their benefits against their drawbacks, and issue strategies for successful adoption and governance of public cloud. While public clouds are cheaper and require less maintenance than the current State Cloud, their limitations concerning privacy, data security, and regulatory compliance are complex. Through the review of modern political decision-making research, an analysis of existing Ministry decisions, and policies within other governmental organizations, we conclude that the Ministry should enact a multi-stage process to the adoption and governance of a public cloud. We recommend a framework by which to secure negotiated knowledge among critical governance actors and ensure stability in the ongoing process. Additionally, we provide elements for agreement among actors with disparate goals, such as the cost of doing nothing or expansion of the negotiating structure within a multi-issue game. We highlight cases for further study in this area, and finally, we provide implementation recommendations and leave the reader with information to consider regarding potential future risks and mitigation strategies.

Guidance for Reading

This report is focused on recommendations to the Ministry of Justice and Security regarding their approach to information management and purchasing with regards to a potential public cloud implementation. It is intended for the Ministry's Office of the Chief Information Officer and focuses on the positioning of public cloud technology within a larger question of governance. Recommendations are issued regarding how the Ministry should move forward and how it can engage stakeholders in the process to ensure a successful implementation.

This report assumes no familiarity with the concept of cloud computing, data storage, or data privacy. For additional information on these topics or the Dutch political environment, please see the list of references at the end of this document.

Index of Contents

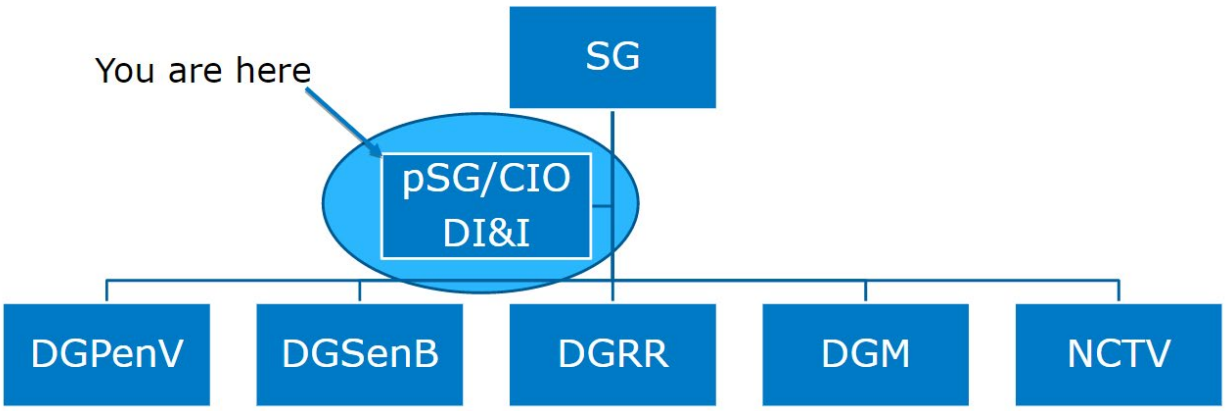
Introduction

Client Overview: The Ministry of Justice and Security

The Netherlands Ministry of Justice and Security is among the largest organizations within the Dutch national government, employing more than 100,000 civil servants across almost 50 sub-organizations. It includes Politie, the national police force, as well as immigration services, the independent but linked judiciary and court system, and many others. It is led by the Minister of Justice and Security, Ferdinand Grapperhaus, who serves as a cabinet member within the Prime Minister's government.

The Ministry is tasked with administering the law, preventing and solving crime, enforcing immigration policy, and overseeing the processes necessary for a just and fair society. It is closely aligned with the Ministry for Kingdom and Interior Relations, with which it coordinates on a variety of domestic policies, as well as the rule of law and the security services.

Within the Ministry's leadership, the Office of the Chief Information Officer (DI&I) oversees technical infrastructure and support for the organization, as well as purchasing. This unit is responsible for supporting and advising the Ministry's internal departments about ICT infrastructure, including the emerging question of how, if chosen, to implement and govern a public cloud.



Organizational Chart of the Senior Ministry Departments

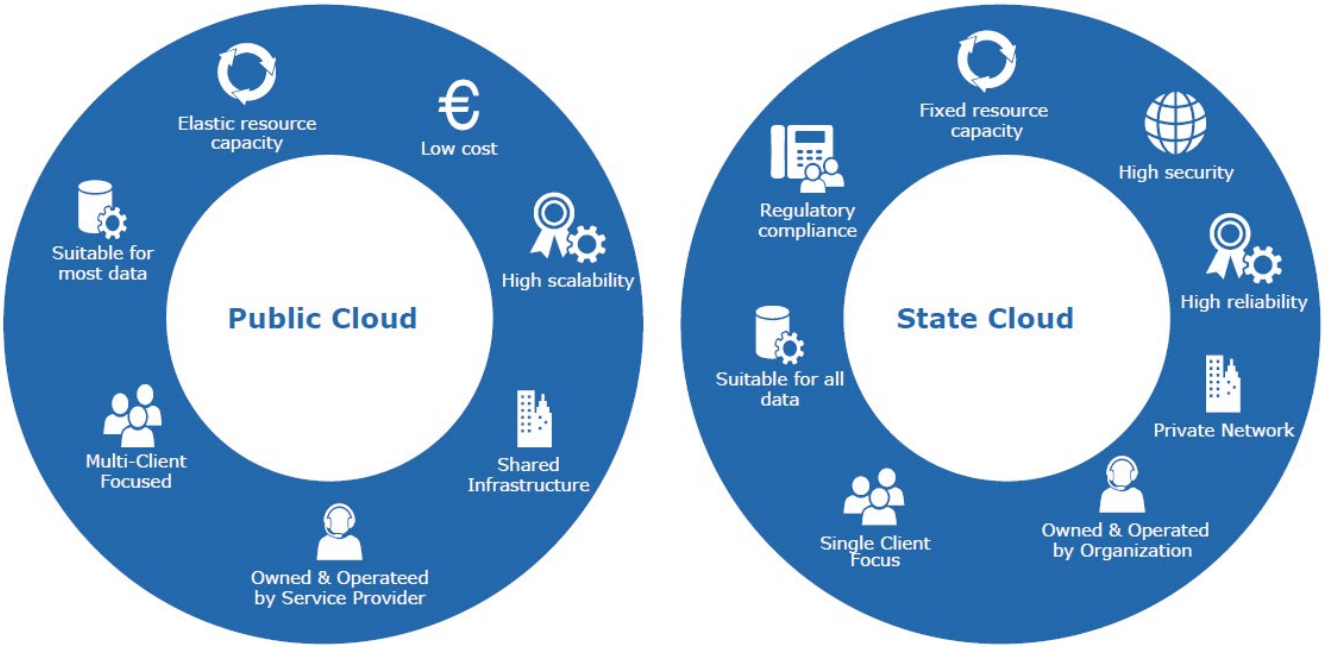
Client Request: Public Cloud Implementation and Governance Assessment

The DI&I, on behalf of the Ministry, seeks to implement a public cloud instance to store Ministry data. This represents a shift from the existing technologies in widespread use at the Ministry and a move towards greater efficiency.

On an individual computer, data is stored on an internal drive. This is referred to as local storage. Within an organization, data may be sent to larger groups of drives owned and managed by the organization that are connected to a user's computer via an internal network - so called "on-premise" storage. This was the first model of large-scale data storage and has been widely utilized by large organizations.

As the cost of data storage and transfer has decreased, major vendors like Microsoft, Amazon Web Services, and Google have offered low-cost storage on servers they maintain at data centers around the world, while certain organizations maintain these centers themselves. This offering is called cloud computing. Within cloud computing, there are three major types: private clouds, in which the organization pays for computer hardware that exclusively stores its own data, public clouds that utilize shared hardware with other customers, and hybrid clouds which combine the two above models. Currently, the Ministry employs a privately owned and managed cloud – known as the "State Cloud" for the majority of its data storage.

Public clouds are among the most commonly utilized methods of large-scale data storage in the modern age. They enable a vendor to divide the overhead costs of hardware and maintenance between customers, while portioning their data within that hardware securely using software. They enable customers to store data at a lower cost with reduced maintenance expense, without requiring them to invest in hardware. Customers enjoy a reduction in necessary technical responsibility, with data storage and transfer managed through a web portal, as well as higher "uptime" – the percentage of time that the data is available and can be reliably accessed. The Ministry of Justice and Security has used a public cloud in limited test cases, and the DI&I has found it beneficial to its goals to reduce costs and increase efficiency.



Features of Public and State Clouds

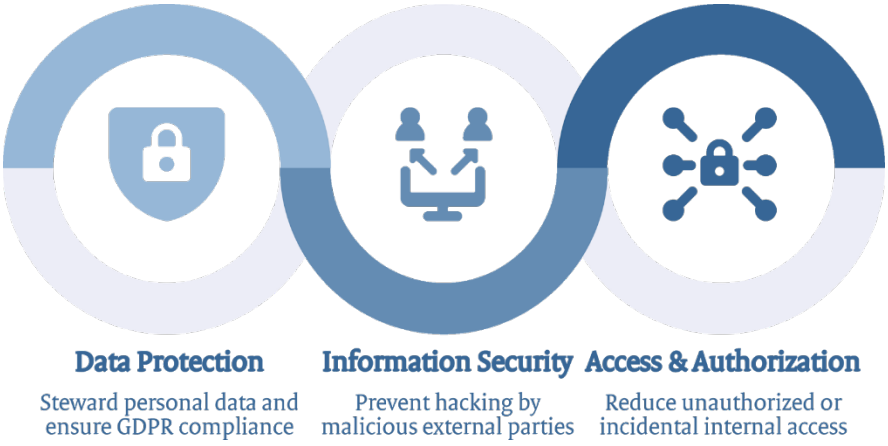
The DI&I seeks to expand the use of public cloud to broad, official application across the Ministry for several reasons. Firstly, a public cloud instance allows for scalability, cost reductions, and decreased maintenance responsibilities that would not otherwise be possible for a single organization to achieve. Using a public cloud service enables the Ministry to add or reduce storage capacity nearly instantaneously, rather than buying hardware through the government's procurement process or depreciating unnecessary infrastructure. As a result, the Ministry can pay for only what it needs, rather than maintain storage year-round for rare moments of peak demand.

Secondly, this reduced cost includes the vendor fee necessary to maintain this storage with highly skilled cloud experts. By utilizing this service, the Ministry avoids the need to employ as many technical experts or be responsible for the maintenance process. These efficiency gains are critical for the organization to most effectively appropriate its resources. Employing a public cloud enables the Ministry to share the cost of the vendor's world-renowned security experts with other customers, rather than maintain its own staff at great expense. Moving away from the current Citrix server State Cloud model reduces the likelihood of a successful cyber attack and enables the Ministry to hold the vendor liable in the event of a breach. With the current Citrix servers, the Ministry itself is liable if recently discovered vulnerabilities in the hardware results in data loss.

Finally, public cloud services represent the future of technical service delivery. Major technology suites such as Microsoft Office and Adobe Acrobat are increasingly sold via subscription and only available through a cloud installation. To maintain access to necessary tools and keep pace with emerging technologies, the Ministry must be able to ensure it has the appropriate infrastructure. Just as the development of word processing and spreadsheet tools demanded a widespread adoption of personal computers, the broad adoption of cloud computing requires organizations develop this capacity as well.

Client Goals: Balanced Scorecard and Outcomes Measurement

To ensure an aligned organizational mission in the implementation of a public cloud, DI&I developed four goals for the evaluation of the process. The first goal is to support internal organizations seeking to move to the public cloud. Through this goal, the Ministry will seek opportunities to help move internal teams onto the public cloud and will provide guidance on how to properly store data. The second goal is to keep control over the data. In order for the Ministry to successfully implement a public cloud, it is crucial that the data being stored in the cloud will not be exposed to data leaks and will be in compliance with GDPR and other policies. This goal also takes into consideration the need to work with vendors to ensure that the data stored in the cloud will not be accessed by individuals to whom the Ministry has not given permission. The third goal is to ensure flexibility and reduce vendor lock-in. As large data storage organizations update their business models, it is important that the Ministry has the ability to set contractual agreements with vendors that minimize reliance on any individual vendor. The fourth and final goal is to proceed responsibly and gain public cloud experience. The Ministry must develop a solid foundation to support a robust public cloud and will need to gather insights from other governmental bodies, IT experts, and legal authorities. The Ministry understands the importance of implementing a public cloud gradually.



The Ministry's Balanced Scorecard

In order to assess the outcomes of their four goals, the Ministry has developed a balanced scorecard comprised of three metrics: protection of personal data and ensuring GDPR compliance, access and authorization, and information security. If they successfully meet their goals, the end result should ensure that all data being stored will only be accessible by relevant parties, that measures are in place to minimize the risk of hacks, and that the data being collected is compliant with appropriate laws. Working through the lens of the balanced scorecard will also help the Ministry proactively select vendors that will be able to meet these criteria as well.

Critical Questions

The Ministry raises several critical questions that must be addressed in order to successfully implement a public cloud. In their request for recommendations, they ask the following:

1. How should the Ministry engage with public cloud providers, who have their own interests and potentially, gain access to highly confidential and critically personal information about Dutch citizens and the workings of the national-scale safety systems?
2. How should the Ministry assess different cloud providers on properties like country of origin?
3. How can the Ministry manage internal and external stakeholders, who have become increasingly concerned about new technologies and corporate access to governmental data?
4. How can the Ministry find a balance between the flexibility and economical gain from cloud services with security and privacy measures?
5. To what extent can the Ministry make decisions on these properties? Is there a need for government-wide standards?
6. How does the public opinion affect the use of certain technologies by governments, and can the Ministry anticipate the political dynamics of public opinion?

In this report, we explore the decision-making environment that shapes these questions, explore potential solutions, and provide impactful strategies that answer the request for recommendations on these topics.

Conceptualizing the Governance Problem

Analyzing Stakeholder Positions

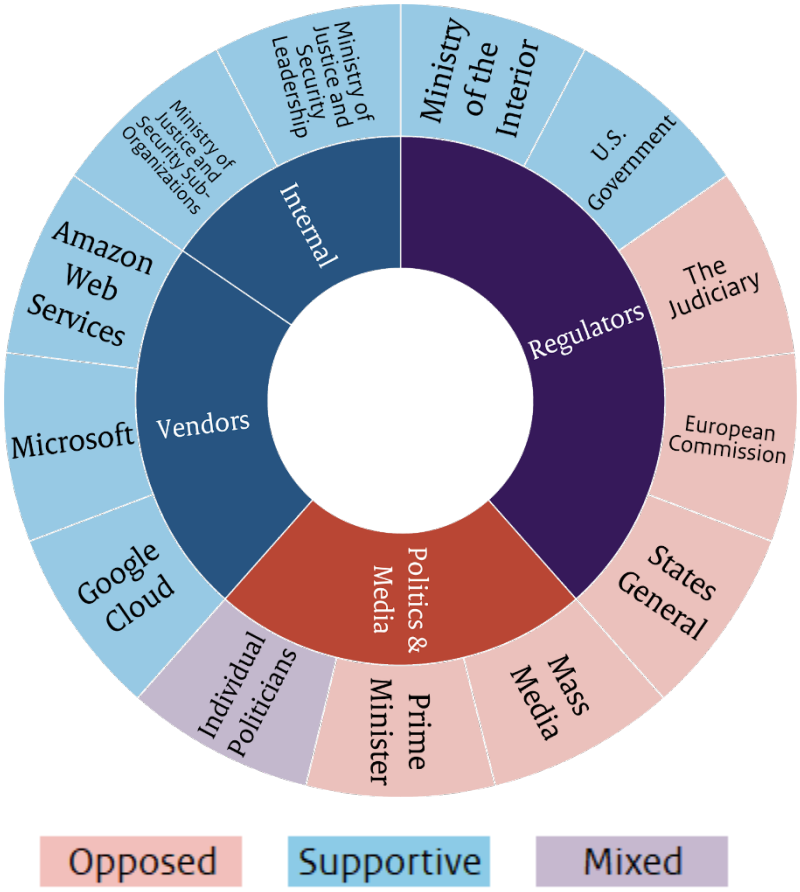
The Ministry exists within a complicated landscape of relevant actors who have a stake in the possible adoption of a public cloud. These stakeholders can be separated into four distinct groups: vendors, internal entities, regulators, and political & media actors. Each of these stakeholders have priorities,

ambitions, and oppositions that affect the adoption of a public cloud at the Ministry, and the power and influence of each group of stakeholders will vary significantly.

Vendors are interested in winning contracts and maintaining business. They will promote lock in and face U.S. regulation. Microsoft is the incumbent, but there are competitors available in Amazon Web Services and Google Cloud. They strongly support the use of a public cloud for their business.

Regulators have little concern for efficiency and seek to ensure compliance with data laws above all else. They may change policies abruptly and have enforcement power over the Ministry. These include European, Dutch, and American regulators due to international data laws like GDPR and the CLOUD Act.

Internal Entities seek to improve the Ministry and secure resources for their own areas of focus. They have a wide range of priorities and require tech support. This includes both leadership and sub-organizations. They will generally value the cost savings of a public cloud, but will be wary of data leaks.



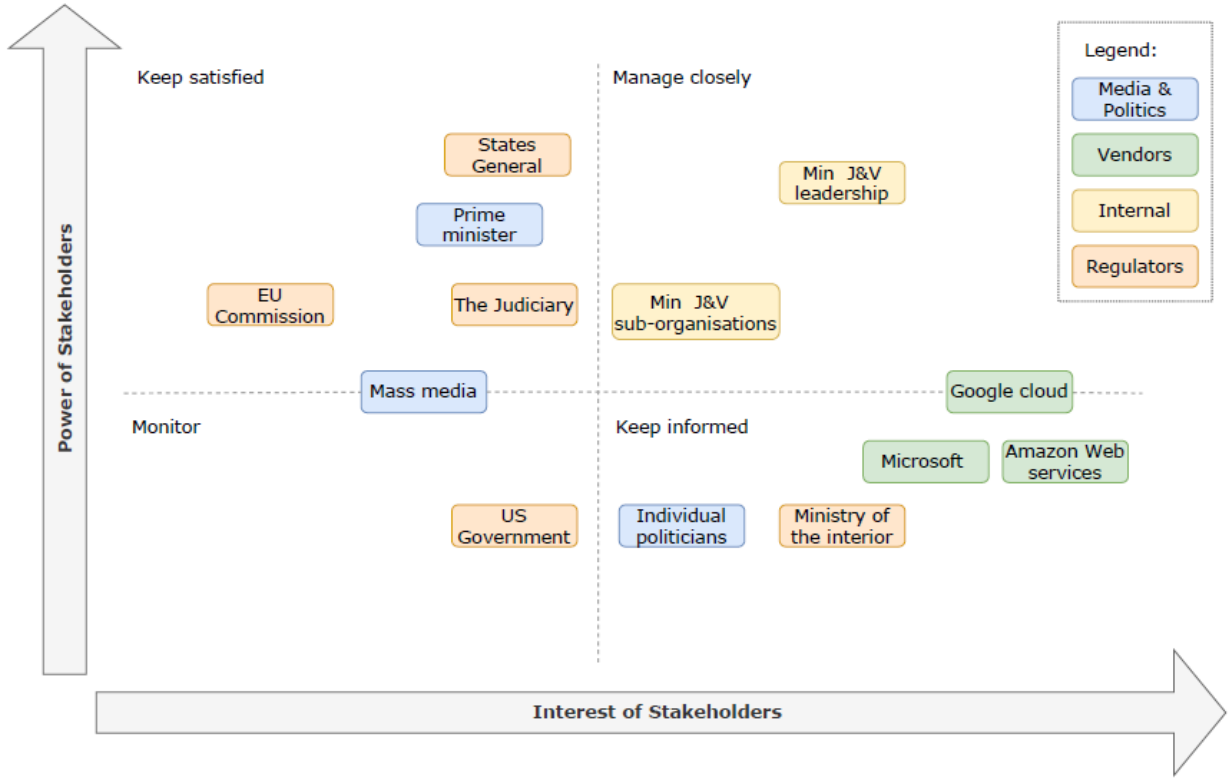
Stakeholder Positions by Group

Finally, **Political and Media Actors** are fluid in their positions on public cloud, but can exert power over the Ministry as those positions change and can cause major shifts in public opinion, such as by highlighting whistleblowers. They are watchful for politically opportune mistakes and are influential to regulators. They have mixed support for any project like this. Due to the varied nature of these groups, some in each group may be for or against public cloud storage and represent varied influence.

Understanding a Wicked Situation

The implementation of a public cloud clearly presents a "wicked problem" and the associated challenge of securing both normative and cognitive agreement from a variety of interdependent actors. Each actor views the idea of a public cloud with varying levels of necessity and prioritizes the potential value or harm to the citizens of the Netherlands differently, meaning that there is no one single problem in the eyes of all the actors. Because there is not a single problem, there cannot be a single solution, and there are too many factors that could impact the success or failure of the solution that cannot be anticipated. Changes by the cloud computing vendor, or to foreign or local laws, public sentiment, or the emergence of other unanticipated challenges might drastically change the efficacy of a solution. The process of implementing

and maintaining any solution cannot be foreseen perfectly. As discussed, these changes will impact different stakeholders in varying ways.



Power and Interests of Key Stakeholders

Deploying a public cloud necessitates balancing the wishes of interdependent actors. DI&I is both regulated by legislatures and enforces policies on sub-organizations. It is beholden to the political will of the Ministry's leadership, while representing trusted technical experts. Certain actors, such as privacy-oriented political parties, may be in total opposition to the project in any form, while other actors will strongly support the expansion of private services to deliver efficient government. Its wicked nature makes it extremely difficult to reconcile the cognitive and normative elements of the decision among the wide range of stakeholders. Therefore, the Ministry must consider cost and effectiveness, evolving legal considerations, public safety, as well as emerging political and social differences to enact this technology successfully.

Defining the Governance Problem

The combination of a wicked problem with a complicated list of stakeholders presents a significant challenge to the Ministry. Public cloud technology has a clear value proposition in terms of efficiency, cost savings, and potential for security management, but risks data leaks and foreign influence. In order to define an effective set of strategies for public cloud adoption and governance, the following problem must be solved:

How should the Ministry of Justice and Security govern the adoption of a public cloud to balance the technology's risks against its benefits for its stakeholders?

Decision Making Analysis

Historical Context

The Ministry of Justice and Security has a complicated history with data storage and citizen perception, which has been exacerbated by rapid changes in public sentiment and regulation. Implementing a public cloud and storing data on hardware not owned by the Ministry would have once been considered unthinkable, especially after the 2011 decision by the coalition government of the Rutte I cabinet to pursue a State Cloud, but now exists as a viable solution popular with several elements of the stakeholder map, particularly given the current Rutte III cabinet's desire to derive value from digitization and lead with technical innovation.

However, two major whistleblowers highlighted incidents of Ministry action deemed inappropriate in 2019, including accusations of bullying in September, and of sexual assault and racial discrimination in December. In early 2020, accusations were shared by a whistleblower that the Justice Inspectorate had withheld information from Parliament on behalf of Ministry leadership. Amidst this, European data regulation under the GDPR as well as the United States CLOUD Act have shaped the legal requirements for data storage and the impact of vendor geography. The importance of this was highlighted in 2019, when a whistleblower shared with the press revelations that Apple had inappropriately accessed Dutch citizen data stored on their servers. Moving forward, the Ministry is extremely cautious to ensure that it is perceived to be acting appropriately and to reduce the likelihood that data is leaked. Given the complicated history of data law, political priorities, whistleblowers, and Ministry perception in the public eye, it is clear that entering the modern decision-making arena requires understanding this context and anticipating rapid changes.

Ministry of Justice and Security Timeline of Key Events

October 1995
EU Data Protection Directive (DPD) enacted

September 2001
Personal Data Protection Act & Dutch Data Protection Authority enacted

Throughout 2011
State Cloud selected by Rutte I

April 2016
GDPR Adopted, replacing DPD

October 2017
Rutte III Cabinet forms, prioritizes digitization

March 2018
US CLOUD Act enacted

May 2018
GDPR Enforceable

August 2019
Apple NL Whistleblower

September 2019
Politie Whistleblower I

December 2019
Politie Whistleblower II

January 2020
Justice Inspectorate Whistleblower

Decision Making Arena

Implementing a public cloud has risks and presents potential regulatory, political, and ethical issues for the Ministry of Justice and Security. It is important to anticipate these concerns in order to move forward with a successful public cloud project.

Regulatory Issues

Most notably, the Ministry of Justice and Security must operate their cloud computing endeavors in compliance with the General Data Protection Regulation (GDPR). This regulation aims to protect personal data within the European Union and the European Economic Area and gives individuals more control over personal data being collected and stored. Per Ministry representative Sander Zwienink in February 2020, DI&I is currently negotiating with incumbent vendor Microsoft to develop a contractual relationship that ensures GDPR compliance. In order to implement a successful public cloud, the Ministry must work with

Microsoft Contract Negotiations Explained

The General Data Privacy Regulation designates multiple levels of responsibility for data storage. There is a measurable difference in liability between a data controller, which decides how data is processed, and a data processor, which merely does the processing. Microsoft had previously labeled itself a data processor, but following a probe from the Ministry moved to label itself a data controller, ensuring stricter liability for data management.

The company's policy changes also include improvements to their Office 365 line of software. These are critical changes for the Ministry, which relies on that software for daily operations as a separate issue from public cloud implementation and governance.

all vendors to ensure that any information stored on the cloud will be compliant with this law. As of 20 February 2020, the DI&I is approximately 80% finished with the Microsoft contract and believes it will be able to secure similar concessions from the other two hyperscale vendors Amazon Web Services (AWS) and Google. The negotiations have so far led to changes in European terms and conditions for all European Microsoft customers, and will likely shape the approach regulators take with AWS and Google.

The Ministry will also need to take into consideration the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, which requires data companies in the United States to release stored data if requested by warrant. Currently, all major vendors that are currently able to provide the Ministry's necessary level of service are all American. Accordingly, it is possible that the U.S. government can lawfully seize or subpoena data stored by U.S. companies, even if it is stored on servers outside the U.S. from foreign clients. The CLOUD Act does include provisions to contest the release of data if it is in violation of a foreign government's data privacy laws, so GDPR regulations could apply in this situation and would need to be reviewed by the Dutch Data Protection Authority. While only American vendors present the size and capability that the Ministry requires, Chinese vendors like Alibaba and Tencent are growing and may present future use cases. For vendor choices from both nations, the impact of foreign data management presents risks and uncertainties that the security services continue to evaluate.

This uncertainty extends to domestic policy as well. The Ministry for Interior and Kingdom Relations traditionally issues policies for internal management within departments of the Dutch government but has not yet clarified any position on the use of public cloud technologies at a national level. Changes to this policy would impact the successful implementation of these technologies within the Ministry of Justice and Security.

Political Issues

The idea of widespread public cloud adoption enjoys significant popularity among elements of the European Union. The European Commission has proposed the European Cloud Initiative (ECI), a large-scale public cloud option initially used for European scientific endeavors but ideally expanded to governments and organizations. Broadly, the European Union is supportive of an expansion of the use of cloud computing in order to drive innovation and European competitiveness. However, the ECI and the aforementioned GDPR both incentivize public cloud solutions based in Europe and seek to limit the influence of foreign corporations on European data, such as the American hyperscale vendors under Ministry consideration.

In the Netherlands, the Dutch government has not yet taken a strong stance on the idea of a public cloud. As discussed above, there is not yet an official policy from the Ministry for Interior and Kingdom Relations on public cloud technologies. Certain political parties, however, do have opinions on the matter. Amidst conversations during the 2011 coalition structuring, VVD and the ruling coalition concluded that a private State Cloud would be appropriate for the requirements of the government's data storage. However, during the development of the Dutch provisions of the GDPR – the Implementation Act 2018 – several of the major parties sought to limit the strictness of its implementation and enact legal proceedings in serious cases only, demonstrating an openness to new data storage rules. These include the VVD, Democrats 66, and Christian Democratic Appeal, while the GreenLeft and Socialist Party sought stronger policies. While there is still some opposition to the concept of public clouds and their perceived threat to data privacy, there has been an expansion in political support for new data policies in the last decade.

Ethical Issues

The implementation of a public cloud also has the potential to raise several ethical concerns that should be taken into consideration by the Ministry. Foremost, the protection of data is critical to ensure that the Ministry is both legally compliant and acting in the best interest of citizens. While the Ministry has made a determination that data below the level of "classified" would be appropriate for the public cloud, it is important to consider how certain types of data may be more personal to people than its classification suggests, and what implications would arise if a data leak occurred. If the Ministry was to have a data leak, it would be important to ensure that the information stored on the cloud could not cause harm to citizens or the government.

The selection of vendors should also be conducted in an ethical manner and in compliance with anti-bribery, vendor selection, and governmental regulations. The size of any public cloud contract has the potential to attract unethical behavior, and the desire to see the project succeed could lead to actors obscuring relevant facts. In the U.S., the federal JEDI cloud computing contract bid process has been rife with malicious behavior among the American hyperscale vendors and should be reviewed ahead of major bids in the Netherlands. Furthermore, it merits consideration if the Ministry should consider a slower implementation to enable a Dutch company to succeed rather than send that business to a foreign company.

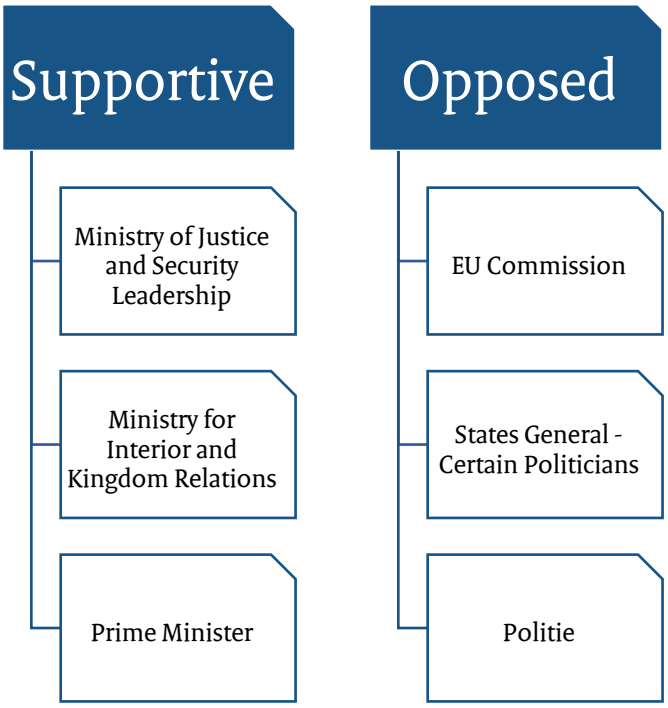
Finally, the Ministry should consider the ethical implications of a public cloud as it impacts potential whistleblowers. The Ministry has experienced several problematic issues with its handling of whistleblowers and the leaking of sensitive information. In light of the potential for widespread data leaks through unauthorized access, an evaluation of the potential good against the risks are necessary. Powerful statements have been made by data leaking whistleblowers like Edward Snowden, demonstrating the potential harm that a public cloud could offer if improperly implemented. Evaluating the ability of the government to store such data and develop a positive culture that precludes the need for whistleblowing is a necessity to succeed in this endeavor.

Critical Governance Actors

Implementing any strategy to move to a public cloud will require the commitment of stakeholders. Certain stakeholders, however, are **critical** – meaning the project cannot survive in the long term without them. This may be because they have political authority, financial or regulatory power, or because their happiness is needed by other critical stakeholders. For the Ministry, some of these are supportive of the project, while other critical actors are opposed.

Supportive

The Ministry of Justice and Security Leadership value the cost savings, efficiencies, and maintenance reductions of public cloud, and are critical because they control the Ministry's budget and actions. Secondly, the Ministry for Interior and Kingdom Relations supports the project because they have set each Ministry to the responsibility of determining their own policy, and that provides a framework for future developments. They are critical because they can introduce new policies and overrule the Ministry. Lastly, the Prime Minister supports the endeavor because it supports his government's mission to be innovative, save money, and lead in digitization. He is critical because his opposition would override any Ministry decisions and move public opinion drastically.



Opposed

The EU Commission is generally opposed, because they will want to avoid using U.S. companies in support of European initiatives and would rather expand European capacity. They have critical impact because pan-European decisions in regulation could drastically impact the standards the Ministry must follow for such a project. Additionally, certain politicians in States General will be opposed for reasons such as data privacy, data sovereignty, or economic competitiveness and could prove critical due to their impact on the government or the Prime Minister. Finally, the recently troubled background of Polite will mean that they are opposed to technologies that have the potential for leaks or security concerns. Their size and political influence, both within and outside the Ministry, means that they can have a significant impact on the project's success or failure.

Strategy and Implementation Assessment

Review of Considered Interventions

Our group explored several strategies that the Ministry could take prior to solidifying our final three-phase strategy process. We decided against the below strategies, as they presented many flaws and potential challenges with implementation, which we have outlined.

1. Decide-Announce-Defend Model

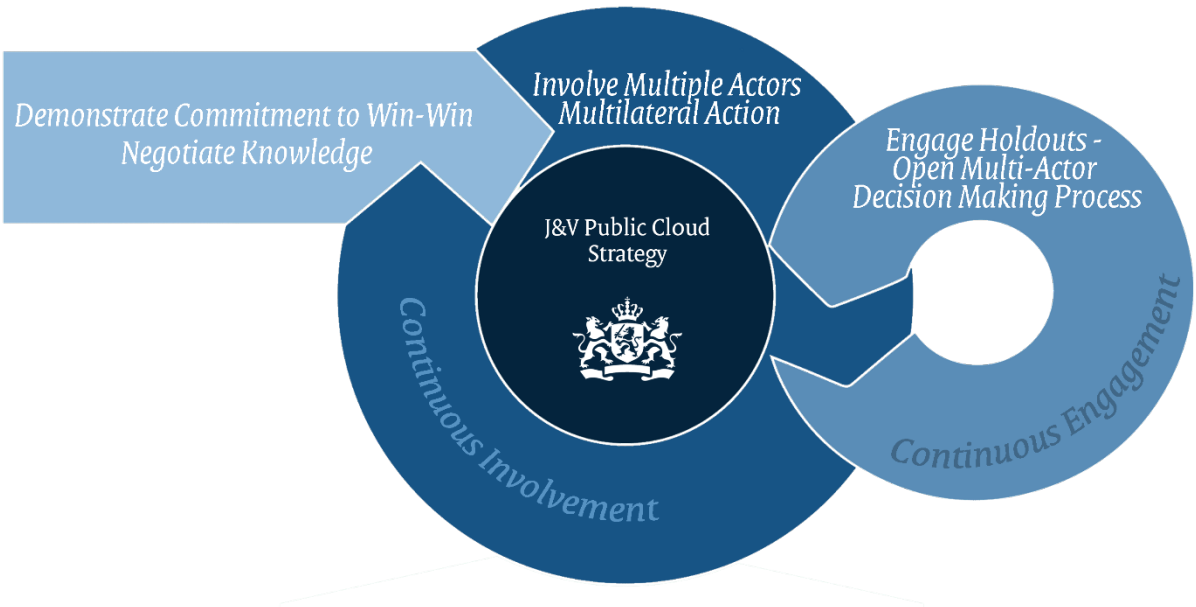
In this strategy, a public cloud would be adopted without the buy-in of relevant stakeholders or other departments and would rely on a unilateral flying start. The Ministry would begin public cloud implementation without the consultation of key actors in multiple stages. This would be the quickest way to move the Ministry towards using a public cloud to store information and individual organizations would have to simply settle for this new reality and update their processes to be compliant with new data storage goals. This strategy would create consideration risk and the potential for data leakage. As the roll-out of the public cloud would be sudden with no input for departments, the Ministry would face issues with incorrect data storage, lack of long-term vision, and backlash from important stakeholders.

2. Break off from U.S. Vendors and cherry pick preferred EU or Dutch vendors
In this strategy, the Ministry would cut ties with Microsoft, Amazon, and Google. As the United States currently has laws in place that concern the Ministry, such as the CLOUD Act, breaking off contracts with these organizations to ease some of the concerns could be an option. If this happens, the Ministry would then need to find an EU-based or Dutch replacement to store data the Ministry would like to put on the public cloud. This strategy provides several potential issues. First, the Ministry already has relations with the U.S.-based vendors and would have to find a way to move all data already stored with these vendors to another vendor at significant expense. Secondly, at this time an EU-based or Dutch-based solution that has the infrastructure and security features in place to compete with the U.S. based companies simply does not exist. The Ministry would have to freeze their ambitions of adopting a public cloud until a vendor that was of the same caliber could be developed.

3. Free-Riding Strategy
In this strategy, the Ministry would allow other organizations within the government to attempt a public cloud implementation before beginning its own. By doing so, the Ministry would be able to learn from the successes and failures of other groups without committing its own capital to the project. However, this strategy is not viable for multiple reasons. Very few other organizations are as large and complicated as the Ministry, and none exist in the same regulatory environment. Relying on others would still require extensive commitment internally and would delay the opportunities for success. This approach would also weaken the Ministry's position in contract negotiations by sacrificing first-mover advantage.

Proposed Strategies and Implementation for Public Cloud Adoption and Governance

Our group recommends that the Ministry of Justice and Security act on three strategies to successfully implement a public cloud and address outstanding organizational and stakeholder concerns. Like most successful strategies, our recommendations rely on multilateral decision making and involving several key stakeholders to be successful. Our strategies also rely on continually engaging with these stakeholders in an iterative capacity to successfully adopt and govern a public cloud.



Strategy Diagram for Public Cloud Implementation

We would first recommend that the Ministry **demonstrate a commitment to win-win by using a negotiated knowledge strategy**. We would recommend that the Ministry develop a J&V Public Cloud Standards Board to govern the creation and evaluation of public cloud information, and to audit vendors over the course of the project. The Ministry will need to ensure that the selection of board members is equitable and is comprised of the most members that will add both technical and political value. We would recommend that the Ministry employ a third-party consulting group that specialized in Information technology strategy that has experience implementing boards of the caliber necessary to meet the requirements of the Ministry's public cloud adoption goals. The Ministry should also seek the advice of senior leadership within the Ministry and gather individuals that have clear experience in administering this kind of entity, as well as subject matter experts. Further, the Ministry should liaise with the Dutch Data Protection Authority to ensure the Board is aligned with changes to Dutch data laws. The development of a board that is trustworthy and accountable will be essential for the continuation of public cloud ambitions at the Ministry. Once established, the Board will need to create a charter and establish accountability for the new public cloud at the Ministry.

In the second phase, we recommend that the Ministry **involve multiple actors through a multilateral action strategy**. Since the Ministry will have developed a Standard Board and conducted a full audit of vendors, we would recommend that negations to ensure GDPR and telemetry compliance are completed with the selected vendors. In order to have public buy-in and be compliant with EU and national laws, this step must be completed to adopt a public cloud solution. Once complete, we would then recommend that the ministry work with individual departments or teams to conduct pilot projects that involve low-risk data. The Standards Board should be utilized here to find teams within their departments that would be good candidates. Lastly, in this phase we recommend that the teams selected work with the Standards Board to conduct training sessions for other departments within the Ministry to get them ready for a full public cloud launch. The pilot teams should also be highlighted in company newsletters, internal town hall meetings, and industry-specific conferences to show that the Ministry is working to successfully launch and serve as a public cloud leader. This will incentivize more internal teams to participate in the public cloud and will also serve as a means to secure buy-in from other ministries and departments within the Dutch government.

Case Study: The Hague Forum for Cloud Contracting

In August 2019, the Ministry for Justice and Security co-hosted The Hague Forum for Cloud Contracting with the European Data Protection Supervisor. They established the EU Software and Cloud Suppliers Customers yearly meeting, where government entities across Europe could share information and discuss how to approach hyperscale vendors like Amazon, Google, and Microsoft.

By bringing together multiple government perspectives to negotiate common knowledge with regards to cloud computing contracts, all parties become more knowledgeable and better prepared to protect private data.

The Standards Board should take key lessons from this forum and model processes based on what was learned when developing the Forum.

In the final phase, our group recommends that the Ministry **engage holdout stakeholders through a multi-actor decision making strategy**. In this phase, we have categorized groups that are apprehensive into two categories: those with aligned goals but specific concerns and those with nonaligned goals who are less willing to consider the project at all. The groups that represent the former can be worked with specifically to understand their pain points and come to a mutual agreement, through the expansion of the negotiating table by creating a multi-issue game. For example, if an actor is concerned with national

security threats, the Ministry should emphasize that vendors have top security capabilities that the Ministry would not be able to maintain independently. By ensuring compliant contractual agreements with vendors and conducting regular audits, keeping data stored with vendors should not prove to be a more effective solution than the Ministry maintaining the safety of the data on its own. Further, for actors concerned with climate change or associated costs of cloud computing being diverted from climate efforts, the Ministry can address these issues by showing that cloud computing can help meet admission standards. Actors concerned with government spending, for example, can be shown that public cloud savings could be diverted to other budget items, such as recession relief. Similarly, the cost of doing nothing can be emphasized – if the public cloud project cannot proceed properly, maintenance costs will rise and software like Microsoft Office will become less effective as a tool of the Ministry's workforce. Offering opportunities to expand upon these related goals creates mutual interest in the successful completion of this project, and encourages buy-in.

Anticipated Risks

As with any new strategy implementation, moving forward with these recommendations presents potential risks. These can be assessed by way of an impact-probability matrix, shown below:

1. Disagreements on Standards Board Membership or Purview

When developing a new board, it is possible that the Ministry will face obstacles when selecting members or the information under its purview, impeding the timeline or efficacy of the decisions.

2. Data Leak or Misuse

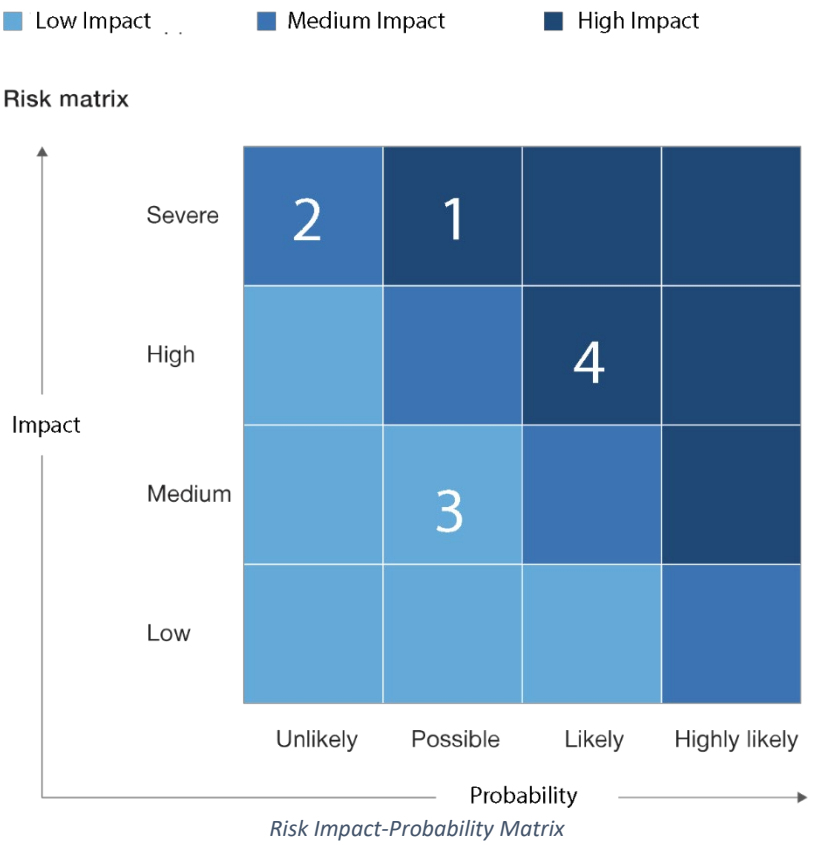
Data leaks or misuse can occur when information is stored on a public cloud, and it is important to keep this in mind. This could be caused by vendor failure or internal actors, and could be intentional or unintentional.

3. Delay in Vendor Compliance with GDPR and Telemetry Laws

Vendors can be slow to implement changes to how they store data, and this could slow the implementation of a public cloud at the Ministry.

4. Changes in Data Privacy Laws

National and international data storage and collection laws evolve quickly, and these changes could impact how the Ministry must work with vendors to maintain a compliant public cloud.



Risk Impact-Probability Matrix

Risk Mitigation Strategies

1. Disagreements on Standards Board Membership or Purview

The Ministry should employ a private consulting company to help establish the Public Cloud Standards Board. This consulting company should have extensive experience developing standards boards for the

adoption of public clouds, preferably with experience in the governmental sector. By using a third-party to develop the board, the Ministry will mitigate bias in the selection process and will ensure that the level of expertise and knowledge necessary to have a successful board is met. Additionally, senior leaders within the Ministry should be consulted with to ensure executive buy-in and determine if certain individuals should be invited to sit on the board to keep senior leadership informed of the board's actions.

2. Data Leak or Misuse of Data stored on Public Cloud
The Ministry should employ data privacy and policy experts to ensure that data leaks or misuse are minimized. A team of cybersecurity experts should conduct full audits of the data being stored on the public cloud regularly. Additionally, trainings should be conducted to help individual departments understand what types of data should be stored on the public cloud.

3. Delay in Vendor Compliance with GDPR and Telemetry Laws
Large organizations that handle cloud storage efforts can sometimes face delays when ensuring their services are compliant with international and national laws. It is important for the Ministry to be persistent in their advocacy for compliance and inform vendors that the lack of compliance could result in no longer doing business with the organization. The Ministry should also push for hard deadlines to be able to inform internal parties of the progress being made by the vendors.

4. Changes in International or National Data Privacy Laws
The Ministry should be abreast of changes going on at the national level with Dutch privacy and data laws. To anticipate these changes, they should regularly consult the Dutch Data Protection Authority and the European Data Protection Board on impending changes to laws. Further, the Ministry should be in close contact with experts and legal teams on international data privacy laws and impending changes. By proactively addressing and anticipating these changes, the Ministry will be better prepared for conversations with vendors and other key stakeholders.

Conclusion

Public cloud technology stands to provide the Ministry of Justice and Security with significant gains in efficiency, cost savings, as well as major reductions in maintenance requirements. While the move to a public cloud presents regulatory, political, and ethical risks, the benefits to the organization outweigh these when properly mitigated by responsible implementation and governance. Amidst a complicated landscape of internal and external stakeholders, the Ministry and its information technology staff must drive the project forward to ensure the organization is able to complete its mission with the best available tools.

The Ministry of Justice and Security should govern the adoption of a public cloud through a three-strategy approach in order to balance the technology's risks against its benefits for its stakeholders. Initially, they would secure buy-in through negotiated knowledge, before proceeding to initial pilot implementation with multilateral action. Finally, holdouts would be engaged and brought into the iterative process to expand the successful use of public cloud within the Ministry without excluding partners or processing recklessly. These holdouts can be engaged by expanding the negotiating table and emphasizing the cost of doing nothing. By utilizing these strategies, the Ministry of Justice and Security will be able to support internal organizations moving to public cloud, keep control over collected data, ensure flexibility without vendor lock in, and gain public cloud experience by proceeding responsibly.

References

Bart Custers, A. M. (2019). Chapter 2: The Netherlands. In *EU Personal Data Protection in Policy and Practice* (pp. 17-47). The Hague: T.M.C. Asser Press.

Bruijn, H. d. (2019). Reflection. In H. d. Bruijn, *The Art of Political Framing: How Politicians Convince Us That They Are Right.* Amsterdam: Amsterdam University Press.

Collins, R. D. (2018, February 6). *H.R.4943 - CLOUD Act.* Retrieved from Congress.gov: https://www.congress.gov/bill/115th-congress/house-bill/4943

Dan Wald, R. d. (2019, May 29). *The Five Rules of Digital Strategy*. Retrieved from Boston Consulting Group: https://www.bcg.com/publications/2019/five-rules-digital-strategy.aspx?linkId=68308829&redir=true

Dutch Siri recordings are being listened to by Apple contractors: Nu.nl. (2019, August 2). Retrieved from DutchNews.nl: https://www.dutchnews.nl/news/2019/08/dutch-siri-recordings-are-being-listened-to-by-apple-contractors-nu-nl/

European Commission. (2019, November 8). *The European Cloud Initiative*. Retrieved from European Commission: https://ec.europa.eu/digital-single-market/en/%20european-cloud-initiative

European Data Protection Supervisor. (2018, May 5). *The History of the General Data Protection Regulation*. Retrieved from European Data Protection Supervisor: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Feldscher, J. (2020, February 13). *Judge orders Pentagon to stop work on JEDI cloud contract*. Retrieved from Politico: https://www.politico.com/news/2020/02/13/pentagon-jedi-cloud-contract-114942

Irion, K. (2012). Government Cloud Computing and National Data Sovereignty. *Policy and Internet*, 40-71.

Jim Boehm, P. M. (2018, November). *Cyber risk measurement and the holistic cybersecurity approach*. Retrieved from McKinsey & Company: https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach

Lomas, N. (2019, November 18). *Microsoft announces changes to cloud contract terms following EU privacy probe*. Retrieved from TechCrunch: https://techcrunch.com/2019/11/18/microsoft-announces-changes-to-cloud-contract-terms-following-eu-privacy-probe/

Magdalena Kaminskae, M. S. (2018, December 13). *Cloud computing - statistics on the use by enterprises*. Retrieved from Eurostat: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises&oldid=416727

Pieters, J. (2019, September 26). *Police Whistleblower on Racism, Bullying Placed on Leave*. Retrieved from NLTimes.nl: https://nltimes.nl/2019/09/26/police-whistleblower-racism-bullying-placed-leave

Pieters, J. (2020, January 28). *Justice Inspectorate Pressured To Withhold Info From Parliament: Report*. Retrieved from NLTimes.NL: https://nltimes.nl/2020/01/28/justice-inspectorate-pressured-withhold-info-parliament-report

PrivacyBarometer.nl. (2018, May 15). *House of Representatives: The Dutch Data Protection Authority should not enforce strict rules*. Retrieved from PrivacyBarometer.nl: https://www.privacybarometer.nl/maatregel/152/Tweede_Kamer_akkoord_Nederlandse_invulling_Europese_privacywet

PrivacyCompany. (2019, August 29). *The Hague Forum for Cloud Contracting*. Retrieved from PrivacyCompany: https://www.privacycompany.eu/blogpost-en/the-hague-forum-for-cloud-contracting

Sander Zwienik, R. A. (2010). Setting the Dutch E-Government Interoperability Agenda: A Public-Private Partnership. In Y. Charalabidis, *Interoperability in Digital Public Services and Administration: Bridging E-Government and E-Business* (pp. 25-39). Hershey: Information Science Reference.

Two police officers arrested for leaking information to the press. (2019, December 19). Retrieved from DutchNews.nl: https://www.dutchnews.nl/news/2019/12/two-police-officers-arrested-for-leaking-information-to-the-press/

Vandekerckhove, K. L. (2018). *The Dutch Whistleblowers Authority in an international perspective: A comparative study.* The Hague: The Dutch Whistleblowers Authority.

Whitton, H. (2001). *Implementing Effective Ethics Standards in Government and Civil Service.* Transparency International.

Zwienink, S. (2020, February 20). Public Cloud and the Ministry of Justice and Security.

Prepared for the Ministry of Justice and Security in April 2020

TU Delft EPA1424 - Political Decision-Making

TU Delft