Dutch central government in the cloud

Dark clouds looming

2025

Netherlands Court of Audit

Contents

1. Executive summary

Audit background and specification

The Dutch central government is increasingly using the cloud to improve its performance and operation. The cloud is a distributed collection of computer servers hosting software and data that can be accessed and processed over the internet. Using the cloud can improve the delivery of public services and increase central government's operational efficiency. However, the cloud also exposes the government to risks regarding digital sovereignty, business continuity and data protection. A cloud service provider can, for instance, agree to another state's request for data, become bankrupt or be hacked.

Central government's effective performance and operation stand or fall on its responsible use of the cloud, taking advantage of opportunities and minimising risks. In the Netherlands Court of Audit's opinion, the government must be aware of and understand its use of the cloud. Ministers and parliament can only promote responsible use of the cloud when these uses are clear, and when the opportunities and risks are known. This report presents the audit performed by the Netherlands Court of Audit and adds to the government's responsible use of the cloud. Our audit covered the use of the cloud at all Dutch ministries to present an overall view on the Dutch central government's use of the cloud.

In 2022, the Minister of the Interior and Kingdom Relations (BZK) relaxed central government policy on the cloud. The use of public cloud was initially not allowed in central government (see following box), but it is now permitted subject to conditions (BZK, 2022). We investigated whether ministries satisfied the conditions in the period October 2023-August 2024. One condition was whether a ministry had full insight into its cloud use and carried out risk assessments.

Central government's use of the cloud must respect 3 principles that underpin its performance and operation for the benefit of citizens and businesses: it must safeguard digital sovereignty, business continuity and data protection. We investigated whether these principles were safeguarded in 3 public cloud contracts.

In the following box, we first explain what the cloud is before summarising our conclusions and recommendations.

What is the cloud?

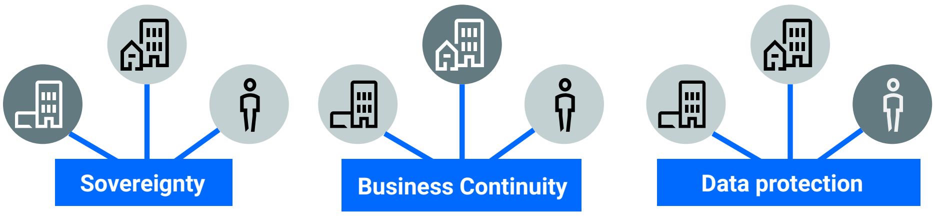
Cloud computing is the use of hardware, software and data over the internet. The physical cloud environment (the hardware) may be located anywhere in the world. If a cloud environment is used by a single organisation, it is known as a private cloud. A cloud environment that is used by more than one organisation is a public cloud. These IT terms should not be confused with the common meanings of private and public when applied to companies and organisations. Large commercial companies such as Microsoft usually offer public clouds, whereas central government service centres tend to offer private clouds. Ministries use public clouds for office automation, for meteorological data systems and for communication with citizens and businesses. The assurances public clouds give regarding digital sovereignty, business continuity and data protection are critical.

What does cloud mean for citizens and businesses?

Office automation for several ministries (e.g. M365 via SSC-ICT)

Meteorological data, e.g. for ship navigation (KNMI)

Sensitive personal data at government healthcare contact centre (CIBG)



Conclusions

We draw the following main conclusions from our audit:

1. The Dutch central government has limited insight into its use of cloud services.
2. Central government does not make appropriate strategic risk assessments.
3. The 3 public cloud contracts we audited inadequately safeguard the principles of digital sovereignty, business continuity and data protection.

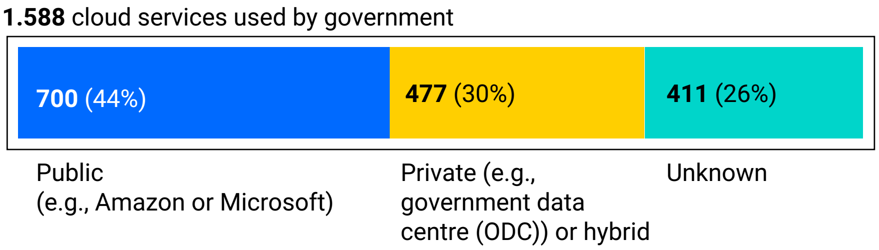
We conclude from the audit that central government has started using cloud services without thoroughly considering the implications and now has weak control of its cloud use. We qualify central government's use of the cloud as **worrying**. The services provided to citizens and businesses, as well as central government's operational continuity, are exposed to too much risk. The potential harm caused by an interruption of public services could disrupt the country and society. Furthermore, because many cloud services are provided by non-EU companies, this topic cannot be seen in isolation from current geopolitical tensions.

Conclusions on central government's use of the cloud

Central government is making avid use of the public cloud

Every Dutch ministry is using public cloud services provided, for instance, by Microsoft, Amazon and Google. These 3 major US companies provide more than half of the Dutch government's material public clouds Of the 1,588 cloud services used by central government, 700 (44%) are public cloud and 477 (30%) private cloud. The ministries do not know whether 411 (26%) of their cloud services are public, private or hybrid cloud, see figure below.

Ministries do not know whether a quarter of their cloud services are hosted on a public, private or hybrid cloud



Limited insight into cloud services

We conclude that ministries have limited insight into the cloud services they use. Enhanced insight into cloud use would strengthen central government's compliance with laws and regulations, use of opportunities, mitigation of risks and fulfilment of disclosure notifications.

Two-thirds of cloud services not risk assessed
We conclude that ministries make insufficient strategic risk assessments before deciding whether to use the public cloud. Of the 700 public cloud services identified, 126 are classified as ‘material’ (i.e., vital to an organisation’s primary task, such as collecting taxes or issuing visas). No risk assessments were conducted for 84 (67%) of these material cloud services. There is therefore a risk that data are not protected and services are open to sabotage. It is difficult for the State Secretary for Digitalisation – through the government’s Chief Information Officer (CIO-Rijk) – to manage interministerial cloud risks.

Limited use of central government expertise and purchasing power
We conclude that ministries have little contact with the central government entities tasked with strategic vendor management (SLM). They accordingly do not make full use of the expertise available within central government to mitigate risks in agreements with cloud providers. Together, the Dutch ministries form the largest IT consuming party in the Netherlands. Using a central buyer such as SLM-Rijk could help increase coherence and consistency in the ministries’ approaches to cloud services.

Differing cloud policies
We conclude that cloud strategies and cloud policies differ from one ministry to another. This diversity makes it difficult for all stakeholders (ministries themselves, central government data centres, cloud providers) to make consistent agreements.

Conclusions on the audit of 3 important public cloud contracts
We examined 3 material public cloud contracts in greater detail. They were substantial contracts for important public services. The 3 selected contracts related to Microsoft 365 at the Shared Service Centre ICT (SSC-ICT), systems operated by the Royal Netherlands Meteorological Institute (KNMI) and the customer contact centre of the Central Information Point for Healthcare Professions (CIBG).[1]

Weak measures to safeguard digital sovereignty, business continuity and data protection
We conclude that the ministries concerned have not taken appropriate measures in public cloud contracts to safeguard digital sovereignty, business continuity and data protection. Central government will therefore be exposed to risks if, for instance, a cloud service provider is hacked. The delivery of public goods and services to citizens and businesses could be disrupted. There is also a risk of personal and commercial data being misused by malicious or state actors.

Weak grip on contractual provisions governing public cloud services

We conclude that the ministries concerned do not have a strong grip on the contractual provisions governing their public cloud services. They do not have a full understanding of or insight into all their contractual agreements. Many public cloud contracts involve a range of parties, including shared service organisations (SSOs) and subcontractors. We found that agreements were complex and laid down in multiple contracts and documents. The ministries had limited understanding of the agreements. This is problematic, particularly because contractual terms and conditions are intended to control risks.

Recommendations

Our main recommendations to all ministers are:

To safeguard the digital sovereignty, business continuity and data security of public services, central government should present itself to the major cloud providers as a single, unified organisation that sets frameworks and rules, mitigates risks and strengthens its position with cloud service providers and other cloud consumers. It must accordingly increase its understanding of its own use of cloud services and assess opportunities, risks and alternatives more critically before and also during its use of the cloud.

Associated secondary recommendations are as follows:

To the Minister of BZK:

1. Make central government cloud policy more uniform and specific, and oversee the policy's implementation:
   - More uniform: by minimising differences between the ministries' policies and, for instance, by making the guidelines on risk management and use of the public cloud obligatory. Study the possibilities to extend central government cloud policy to local authorities and autonomous administrative authorities (ZBOs).
   - More specific: by, for instance, identifying services that may never be hosted on a public cloud.
2. Improve the organisation of central government cloud policy. Compliance with central government cloud policy is too often a matter of individual choice. On behalf of the State Secretary for Digitalisation, CIO-Rijk should proactively promote the cloud policy in close cooperation with ministerial CIOs, procurement officers and other relevant experts.

3. Ensure that all ministries improve their insight into the cloud services they use and, where risk assessments have not been made, assess the risks of material public cloud services.

To all ministers:

1. Encourage joint procurement and contract negotiation and promote the performance of audits. A central strategic vendor management entity (central buyer) could make the conclusion of cloud service contracts more efficient. In an EU context, there is an opportunity for central government to collaborate on the standardisation, certification and enforcement of GDPR conditions. Central government should consider whether there are realistic EU alternatives in combination with a practicable exit strategy.
2. Assess the opportunities and risks of every new potential cloud service, and update the risk assessments of cloud services already under contract. Opportunities and risks differ from one service to another. Assessments should in any event consider the 3 principles of digital sovereignty, business continuity and data protection. Other aspects to consider include cost, innovation capacity and the required know-how and expertise.
3. Improve insight into use of the cloud and, where risk assessments have not been made, assess the risks of material public cloud services. Take risk mitigation measures, for example by agreeing supplementary contractual conditions and checking compliance.

2.
About this audit

This chapter presents the background to the audit, its specifications and the audit questions and activities. It closes by explaining the structure of this report.

2.1 Reason for this audit

Central government is making more and more use of the cloud to improve its performance and operation. The cloud can improve central government's service delivery and increase its operational efficiency. Cloud use, however, also exposes central government to sovereignty, continuity and data protection risks. To perform and operate effectively, central government must use the cloud responsibly, benefiting from the opportunities and controlling the risks. Insight into how the cloud is used is essential. The audit objective is to improve insight into central government's use of the cloud and to check whether central government lives up to its own standards, for instance by carrying out risk assessments. Only if it is known how central government uses the cloud and what the opportunities and risks are can ministers and parliament use the cloud responsibly. This audit by the Netherlands Court of Audit adds to central government's responsible use of the cloud.

2.1.1 Development of the cloud and central government policy

Central government is increasingly using the cloud. The cloud has many potential benefits, from efficiency and flexibility to scalability and security. It can improve service delivery and increase operational efficiency. Advances in IT are also pushing users such as central government towards the cloud. Microsoft 365, a popular office application, for example, is available in the cloud. Software developers and IT providers are investing less, if at all, in non-cloud solutions. Partly for this reason, the

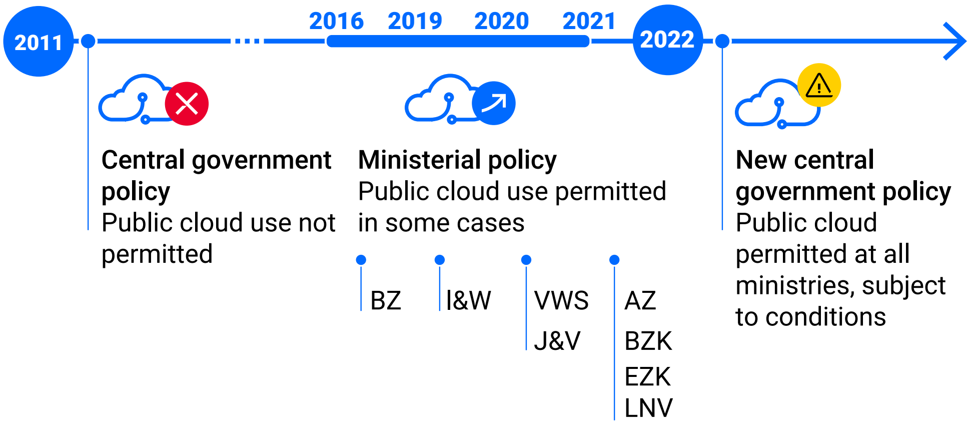
Minister of the Interior and Kingdom Relations (BZK) renewed central government's cloud policy in August 2022. Since then, ministries have been allowed to use public clouds offered by Google, Amazon, Microsoft and other providers subject to certain conditions. For example, a ministry must have a cloud policy, an insight into its cloud use, perform risk assessments and protect personal data.

Public cloud policy: ministerial versus central government

Central government policy has permitted the use of public cloud services since August 2022. Before then, however, more than half of the ministries had already drawn up their own cloud policies and permitted their use of the public cloud.

Figure 1 *Timeline of public cloud policy*

Use of public cloud was not permitted within Dutch central government before 2022


2011
2016
2019
2020
2021
2022
Central government policy
Public cloud use not permitted
Ministerial policy
Public cloud use permitted in some cases
BZ
I&W
VWS
J&V
AZ
BZK
EZK
LNV
New central government policy
Public cloud permitted at all ministries, subject to conditions

Several ministries told us they had developed their own independent cloud policy to meet the growing demand for public cloud services in a controlled manner. They had often been forced to use public cloud in response to changing needs and supply-side changes made by providers. Providers were increasingly offering their applications, such as some SAP applications (enterprise resource planning software), exclusively over the public cloud. The ministries felt they were being pressurised into using the public cloud.

2.1.2 Key principles and risks

Cloud use is not without risk to the fundamental principles of digital sovereignty, business continuity and data protection. The risks can be described as:[2]

- Digital sovereignty: central government must own its proprietary data, including data on citizens and businesses. Data processing systems must be auditable. It must be known who has access to the data and how the data are used.
- Business continuity: public services must be deliverable without being overreliant on IT providers. It must also be possible to use and/or transfer services to different providers.
- Data protection: central government must be able to guarantee that cloud providers adequately protect confidential data on central government, citizens and businesses.

Appendix 4 includes a more detailed, more complete description of these principles.

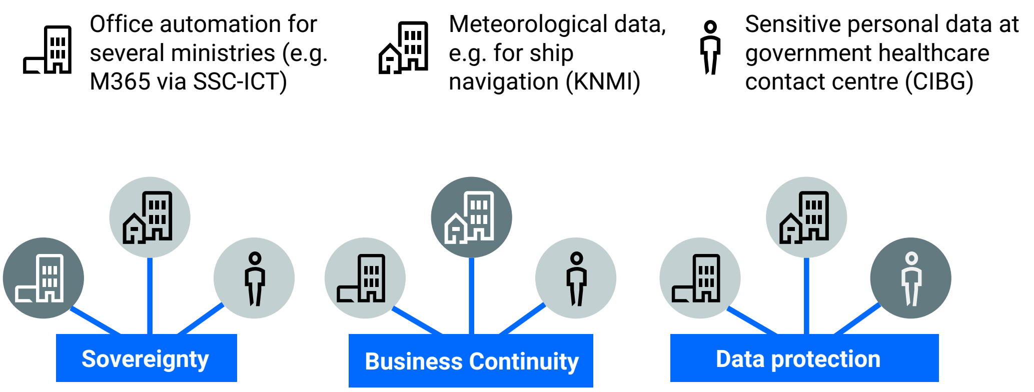
The risks attaching to these principles are real and significant. They are illustrated by the Chinese hack of Microsoft 365 in September 2023, when 60,000 emails were stolen from the US Department of State,[3] and the theft of the contact details of all 65,000 police personnel in the Netherlands in September 2024.[4] The continuity of large IT providers is also uncertain. Atos, an IT provider that is central to several essential central government processes, for example, recently faced potential bankruptcy.[5] Following an evaluation of the central cloud policy, the Central Government Audit Service (ADR) warned against the risk of overreliance on cloud providers (ADR, 2024). It also noted that Microsoft 365 was a 'threat magnet'. This workplace software is used by nearly all of central government in the Netherlands, as well as many foreign governments and businesses worldwide. Its very large and confidential databank is a key motive for state and other malicious actors to exploit weaknesses and attack Microsoft 365.

Risks are ever-present when IT services are outsourced but they can be of a different order when the cloud is involved. Sometimes, databases with information on citizens and businesses are hosted in full by a cloud provider. It is then crucial to know where the data are located geographically, who can access them and whether they can be transferred to another provider. The more remote the IT (which is always the case with the cloud), the greater the risk.

This audit investigates very specifically whether measures are in place to ensure the principles are safeguarded for essential public services. We have examined the ministries' office automation, meteorological data systems and systems to communicate with citizens and businesses.

Figure 2 *Cloud services for citizens and businesses*

What does cloud mean for citizens and businesses?



Office automation for several ministries (e.g. M365 via SSC-ICT)

Meteorological data, e.g. for ship navigation (KNMI)

Sensitive personal data at government healthcare contact centre (CIBG)

2.1.3 Audit objective

The aim of this audit is to gain an insight into the Dutch central government's use of the cloud and to determine whether it meets its own conditions. We also asked whether central government's use of public clouds respected the 3 principles of digital sovereignty, business continuity and data protection. It is essential that parliament knows this. Ministers and parliament can then bolster central government's responsible use of the cloud.

This audit reveals where improvements can be made in policy and implementation, and recommends ways to strengthen risk control and central government's responsible use of the cloud. As the Netherlands Court of Audit, we are thus adding to central government's learning capacity and improving its performance and operation.

The audit questions and activities are presented in appendix 1.

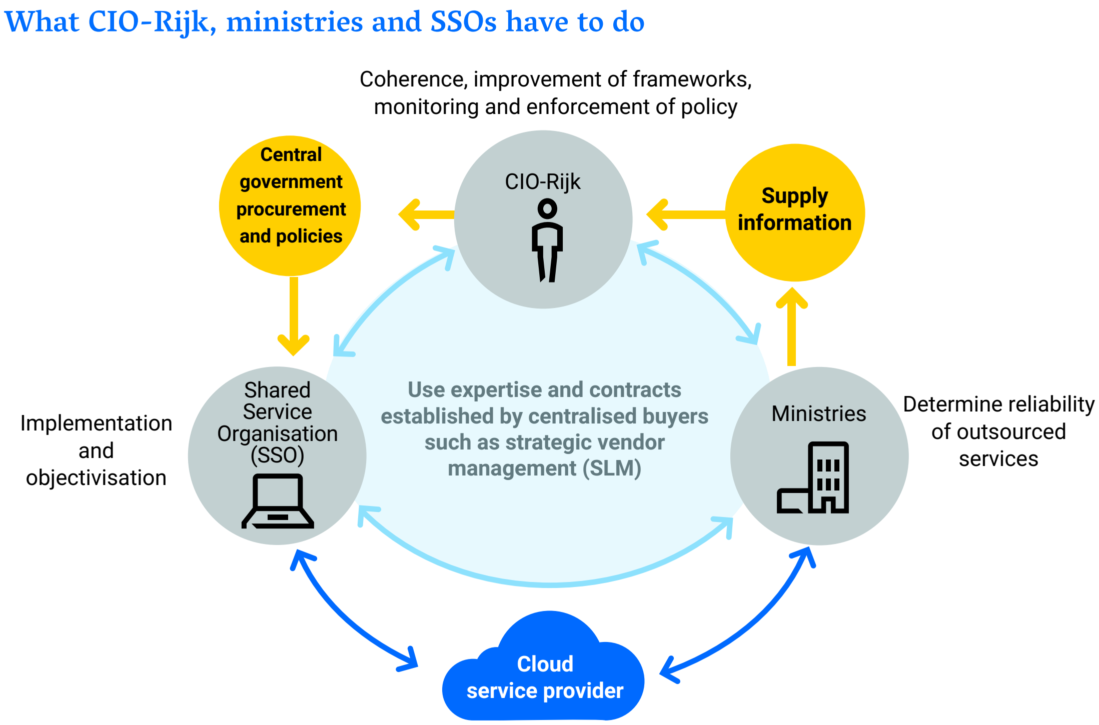
2.2 Central government cloud policy: actors and scope

This section briefly explains the actors concerned and the scope of central government cloud policy. This information is relevant to put our audit findings in context.

2.2.1 Actors involved in central government cloud use

The following actors are involved in central government's use of the cloud. Most of them are also named in central government cloud policy and the associated implementation framework. The actors' responsibilities are laid down in the policy. They are presented in relation to each other in figure 3. The actors are considered in more detail after the figure.

Figure 3 *CIO-Rijk's tasks and responsibilities for cloud services*


What CIO-Rijk, ministries and SSOs have to do
Coherence, improvement of frameworks, monitoring and enforcement of policy
Central government procurement and policies
CIO-Rijk
Supply information
Implementation and objectivisation
Shared Service Organisation (SSO)
Use expertise and contracts established by centralised buyers such as strategic vendor management (SLM)
Ministries
Determine reliability of outsourced services
Cloud service provider

Chief Information Officer-Rijk: CIO-Rijk, a department of the Ministry of BZK's Directorate-General for Digitalisation and Central Government Organisation (DGDOO), promotes the optimal design of central government's computerisation and ICT. The State Secretary for Digitalisation and Kingdom Relations ('the State Secretary for Digitalisation') sets and oversees frameworks via CIO-Rijk.

Strategic vendor management (SLM): Central government's strategic vendor management (SLM) entities formulate contractual provisions and procurement terms for software and cloud services that are laid down in master agreements with IT providers. Ministries and agencies may use the master agreements but are not obliged to do so.

Together, the Dutch ministries form the largest IT consuming party in the Netherlands. Using a central buyer such as SLM-Rijk can help increase coherence and consistency in the ministries' approaches to cloud services.

There is more than one SLM entity. The Minister of Justice and Security (J&V), for example, is responsible for cloud service agreements with Microsoft, Google Cloud and Amazon Web Services. Through its ICT Services unit (DICTU), the Minister of Economic Affairs (EZ) is responsible for Oracle, and the Minister of Finance's Tax and Customs Administration is responsible for cloud agreements with IBM.[6]

Ministries: ministries (and their agencies) are the contracting authorities for IT services that are outsourced, such as the cloud.

Shared Service Organisations (SSOs) and central government data centres (ODCs): SSOs (e.g., SSC-ICT and DICTU) and ODCs (e.g., ODC-North and ODC-Tax and Customs Administration) provide IT and cloud services to the ministries. They provide either their own private cloud services or act as intermediaries with public cloud providers such as Microsoft.

Cloud service providers: cloud services are hosted by many parties, including SSOs and ODCs. Most cloud services (67%), however, are provided by 3 major vendors from the United States: Amazon (Web Services), Microsoft (Azure) and Google (Cloud Platform).[7] Delos Cloud in Germany and Bleu and OVHcloud in France are examples of European initiatives. Service providers in the Netherlands, too, offer cloud environments. Several providers are members of the Dutch Cloud Community, an industry association. The Minister of J&V is a consumer of one such provider, Crayon.

2.2.2 Scope of central government cloud policy

Central government cloud policy states (p. 2):
'Public authorities that are not part of central government are advised to adopt this central government policy. Ministries are encouraged to disseminate it among autonomous administrative authorities and other organisations that report to their minister.'
Local authorities and autonomous administrative authorities (ZBOs) are therefore not subject to the policy. However, central government cloud policy restricts the use of certain databases they keep or administer, which in principle may not be hosted on the cloud. The Ministry of Defence also falls outside the policy's scope. It believes central government cloud policy is not appropriate for a security organisation. We nevertheless investigated whether the Ministry of Defence had a cloud policy and strategy, oversaw its cloud use and carried out risk assessments. We did not investigate one specific standard of central government cloud policy (consultation with strategic vendor management entities).

Central government cloud policy is ‘obligatory’ for organisations within central government, as is the Cloud Risk Management Implementation Framework (‘the implementation framework’). The latter refers to voluntary guidelines (p. 4): *‘Besides the cloud policy and implementation framework, there are voluntary guidelines on risk management and use of the public cloud. They provide practical guidance on how to manage risks. The CIO Board has adopted and periodically updates the guidelines.’*

2.3 Structure of this report

We begin in chapter 3 with an introduction to the cloud and its opportunities and risks. It is based on professional literature and expert interviews. The following 2 chapters describe our audit findings on policy, oversight and assessment and look at 3 specific cloud contracts. We end with conclusions and recommendations and close the report with the state secretary’s response and our afterword.

The report uses the new names of the ministers and ministries as of 2 July 2024. Some ministers do not have their own IT service but use the services of other ministries. The Ministry of Asylum and Migration (A&M) uses the services of the Ministry of J&V. The Ministry of Housing and Spatial Planning (VRO) uses those of the Ministry of BZK and the Ministry of Climate Policy and Green Growth (KGG) and the Ministry of Agriculture, Fisheries, Food Security and Nature (LVVN) use the Ministry of EZ’s. We present findings on 11 ministries, for which several ministers are responsible.

3.
An introduction to the cloud

This chapter describes a number of aspects of cloud computing that put our audit into context. We begin with ‘cloud push’, describe different kinds of cloud and their opportunities and risks and then look at digital sovereignty.

3.1 The advance of the cloud: the cloud push

Cloud computing is the use of hardware, software and data over the internet. There are several reasons for its growing popularity. Advances in IT are pushing users such as central government towards the cloud. Some new products, such as brainstorming software and video conferencing software, are only available in the cloud. Secondly, IT providers are developing and providing services exclusively for the cloud. This is true of some SAP applications used by ministries in the Netherlands. A central government organisation then has 2 options: stop using the service or embrace the cloud. Non-cloud alternatives often cannot be sourced and, moreover, it is often challenging to find staff for maintenance. As a result, organisations are being forced onto the cloud.

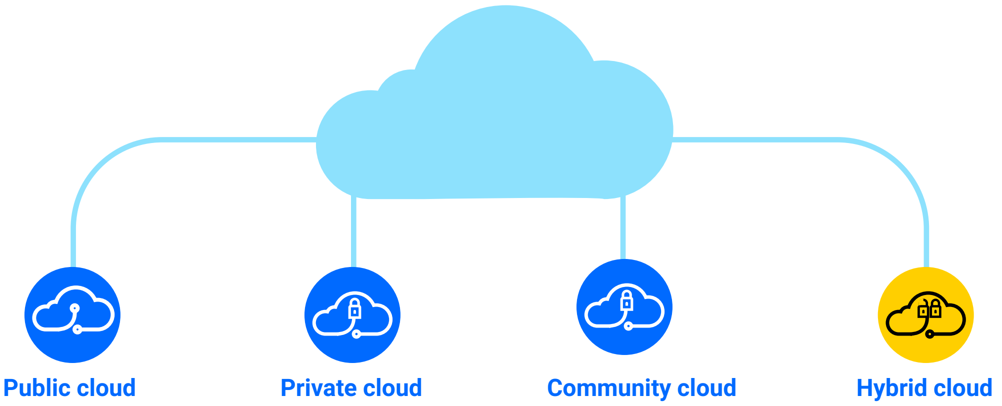
This push towards the cloud should not be underestimated but the decision to use the cloud is sometimes taken too lightly. The experts we interviewed, as well as the Clingendael Institute, pointed out that central government organisations made little effort to find alternatives to cloud services (Clingendael, 2024a). This can lead to ill-considered cloud use.

3.2 Types of cloud

An organisation working in the cloud uses the internet-based services of a cloud service provider (CSP) and does not manage the IT itself. There are several types of cloud.

Figure 4 *Different types of cloud*

There are different types of cloud



The main differences are:

- **Public cloud**: used by multiple parties (in some cases by everyone, both privately and commercially).
- **Private cloud**: used exclusively by a single organisation.
- **Community cloud**: used exclusively by a specific community.
- **Hybrid cloud**: a mixture of the public and private (and/or community) cloud. The IT on a hybrid cloud is a combination of 2 or more interconnected IT environments (private, community or public).

Appendix 4 presents a more detailed, more complete definition of cloud computing and the different forms it can take. We do not consider the community cloud in the remainder of this report; it is not referred to in central government's cloud policy.[8] Furthermore, the report contains few references to hybrid clouds.

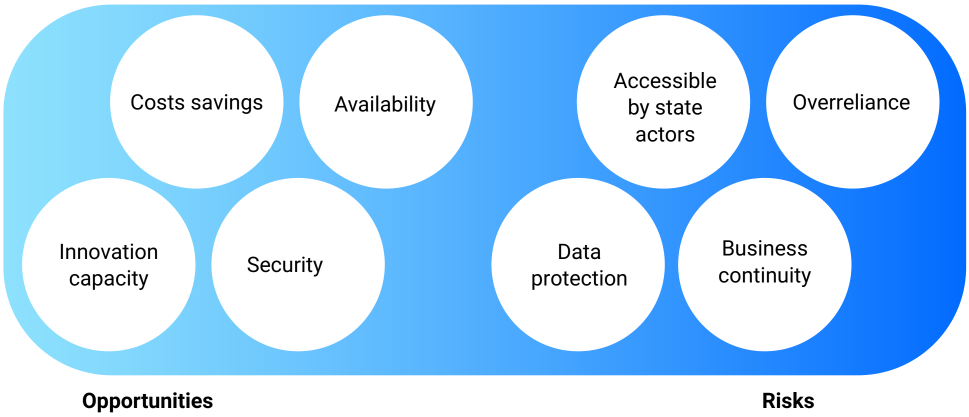
3.3 Cloud opportunities and risks

Working in the cloud presents opportunities, also for central government, such as cost savings and greater efficiency, availability and accessibility, security and privacy and innovation capacity. At the same time, there are risks to digital sovereignty, business continuity and data protection.

The ability to maximise the opportunities depends on the circumstances. Opportunities can turn into risks if central government's assessment of a cloud service is inaccurate, for instance if it does not allow for increases in licensing fees. Conversely, a risk can become an opportunity: data that are not stored in a country's jurisdiction can strengthen sovereignty during a war. The opportunities and risks described in the following sections should be seen in this light.

Figure 5 *Opportunities and risks of the cloud*

Opportunities and risks: depending on requirements and type of cloud, opportunities can become risks and vice versa



3.3.1 Opportunities

Cost savings and efficiency

The public cloud in particular allows central government to provide digital services faster and at lower cost. With a public cloud, central government can rapidly scale up capacity at the touch of a button whenever necessary, without needing its own server capacity. If demand for public services falls, it can reduce the capacity it hires from the CSP. Central government then does not pay for server capacity it does not use. With a public cloud, central government can minimise its own IT infrastructure and reduce management costs. Central government must always remain alert, though, to contract costs and licensing fees, procure only those functionalities it actually needs and be aware of price movements.

Availability and accessibility

Another advantage is the improved availability and accessibility of cloud services. Capacity and bandwidth can be adapted at the touch of a button if not automatically, thus reducing the risk of a website or service going offline. In addition, cloud use makes it easier to collaborate with others, both with other ministries and with international partners.

Security and privacy

The Court of Audit has been investigating IT security and digital privacy every year for at least a decade, and has consistently found many shortcomings in information security, IT management, privacy protection and similar aspects. Ministries are dependent on the expertise available within their own organisations. These risks are also present in the cloud (see AP, 2022 and 2023; CSR, 2021; ICTU, 2024 and NCSC, 2021), but the experts we interviewed at NCSC, ODC-North and other organisations claimed that use of the public cloud could in fact improve the security of services. The big tech companies have invested a lot in IT security expertise. They are in a better position to sustain expertise at a high level owing to their large scale. Good security, moreover, is essential from a commercial point of view: large cloud service providers cannot afford to have the media expose a major data leak.

As noted above, opportunities can become risks. In § 2.1.2 we referred to the ADR's warning that data concentration at one supplier (for example, if only Microsoft is used) increased the risk of hacking and data theft (ADR, 2024).

Innovation capacity

The cloud is also an opportunity to strengthen an organisation's innovation capacity. Many current and future innovations, such as artificial intelligence (AI), are based on cloud technology. Using such innovations and sharing knowledge of them can improve central government effectiveness.[9]

Opportunities based largely on assumptions

The opportunities named above are based largely on assumptions. Organisations consider opportunities to be a given, or a reason to use a public cloud. However, they have not assessed whether a cloud service will be beneficial in a particular scenario or setting. It is difficult to measure whether the opportunities will live up to expectations. This is particularly true of the long-term benefits to a government. The cost savings that businesses have enjoyed cannot be simply transferred to central government. Central government operates in a different setting, with different demands and from a different position. The Dutch central government, for instance, has far more experience and expertise in inhouse IT than in external cloud services.

3.3.2 Risks

Besides opportunities, the cloud exposes central government to risks.

Digital sovereignty: overreliance on providers

By using more and more public cloud services, central government can become overreliant on dominant, monopolistic providers. Most of the providers, moreover, are located outside the European Union (EU) or European Economic Area (EEA). The asymmetric power balance between CSPs and their client central government organisations has arisen because central government organisations do not always have the capacity, expertise and professionalism necessary to keep a firm grip on the cloud and mitigate the risks.

Digital sovereignty: accessible to state actors

CSPs in the US are obliged to provide data to the US federal government. For more information on this risk, see § 3.5.

Business continuity

Unlike many other products that central government procures, it is far more difficult for central government to switch from one CSP to another. To avoid vendor lock-in, organisations must take measures that enable them to use data stored on one cloud on another cloud operated by a different provider.

Data protection

Data stored by a CSP in the cloud are more remote than if they were stored by an organisation's own IT facilities. Authorisation management (who can access the data) is therefore critical. Unauthorised access to the data can result in data theft, manipulation or deletion. The contract with the CSP must state that other cloud users must not be able to access data. There is also a risk that personal data will be incorrectly placed in the cloud because not all organisations know what data may be stored in the cloud.

Limited knowledge and expertise

According to the experts we interviewed, some cloud consumers have too little knowledge of the cloud. Central government is no exception; it is used to outsourcing tasks and exercising only oversight. More outsourcing generally means less inhouse expertise. This limited knowledge can lead to poor risk analyses and weak risk control.

3.4 The meaning of ‘digital sovereignty’

Digital sovereignty is an important concept in this report. It is often raised in discussions of the cloud (Clingendael, 2024a; CSR, 2021; Moerel & Timmers, 2020).[10] References in this report to sovereignty refer to digital sovereignty. We define it as follows:

Digital sovereignty is the ability to take autonomous decisions and actions on essential digital aspects of the economy, society and democracy.[11]

Sovereignty relates to the use and design of digital systems, the data they generate and store, and related workflows. Our control framework breaks down the concept into specific criteria, including:

- *Dataflows and locations*: it is known where the data are located.
- *Publication of data*: agreements have been made on the transmission of data to non-EEA countries.
- *Right to audit*: the right to audit can be exercised in practice.
- *Interoperability*: the system can work with other IT systems so that data can be automated, shared and processed elsewhere.
- *Portability*: the data can always be accessed by the consumer (in this case, central government) and transferred to another CSP, and there is a realistic exit strategy. This prevents overreliance on a single CSP.

According to the experts, sovereignty is often given as a reason to keep data in the country or in the EU and not to use the services of US CSPs. Some countries, however, have deliberately chosen to store central government information in data centres in other countries, see box below.

Sovereign thanks to the cloud, examples from Estonia and Ukraine

Estonia. Estonia has been storing state information outside its own jurisdiction since 2015. The 'data embassy' in Luxembourg is a guarantee that Estonia's critical public services and sensitive state information will be backed up if the country is physically invaded.[12] Use of the cloud ensures that Estonia can continue to function as a state, even if it is at war.

Ukraine. Shortly before Russia invaded Ukraine, the Ukrainian government uploaded its most important data to the cloud. Government data centres have been attacked or disabled by cyberattacks many times during the war. The transfer to the cloud has kept critical information out of enemy hands. Ukraine is now actively backing up government databases in other countries so that public services can be continued during the war.[13]

In these examples, reliance on the countries hosting the data has increased. Nevertheless, Estonia and Ukraine prefer this. Digital sovereignty decisions depend on the context.

3.5 US legislation: access to data

One of the main risks to digital sovereignty is that a foreign security service can request data if the cloud service is provided by a foreign CSP. The CLOUD Act, for instance, gives the US government far-reaching powers to access personal data on EU citizens. The Chinese government has passed similar legislation to obtain access to commercial data. There is therefore a risk that foreign security services will access sensitive government data. As the Dutch central government uses mainly US CSPs, in this section we explain the situation with US CSPs. The US can formally access the data stored on US cloud servers, even if the servers are located in Europe.

3.5.1 US laws and EU treaties

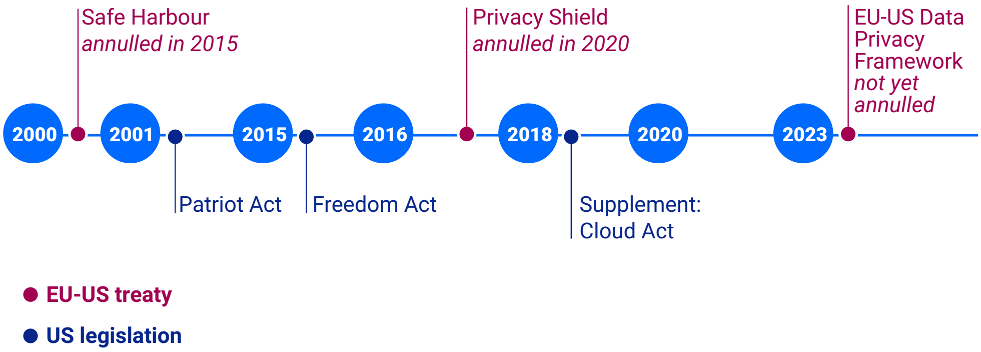
Under the CLOUD Act, US investigation and security services can request data from US CSPs such as Microsoft, Google and Amazon even if the data are stored in a foreign jurisdiction. The EU and US have repeatedly made agreements to control this risk but the European Court of Justice has repeatedly annulled them. This is considered further in the box below. As a result, the US has formal access to the data, even if the servers are located in Europe.

Going round in circles: US laws and EU treaties on data disclosure requests

There have been many international developments in cloud laws and regulations over the years. Figure 6 shows a timeline of cloud-related US laws and EU treaties.[14]

Figure 6 *Timeline of US laws and EU treaties on data protection*

US legislation toned down by EU treaties that then annulled



US legislation

- *2001: the Patriot Act*. This US law came into force in 2001 following the 11 September 2001 terrorist attacks. It extended the US authorities' power to request and collect data.
- *2015: the Freedom Act*. The Patriot Act was replaced with the Freedom Act in 2015. Under the Freedom Act, US authorities can request data from US organisations that are subject to US law. They can also request data that are stored abroad by organisations that have ties with US organisations and that are authorised to install equipment or software there.
- *2018: the CLOUD Act*, a supplement to the Freedom Act. Under the CLOUD Act, US investigation and security services can request data from US CSPs (such as Microsoft), including data located outside the US. The CLOUD Act therefore gives US intelligence services access to personal data in the EU that are processed by US CSPs.

EU treaties

- *2000: Safe Harbour.* The international Safe Harbour Privacy Principles were introduced in 2000. They allowed US businesses to declare that they respected EU privacy rules. The European Court of Justice annulled the Safe Harbour principles in 2015 owing to concerns about US surveillance.
- *2016: Privacy Shield*. The Privacy Shield replaced the Safe Harbour principles with a view to protecting the rights of EU citizens and improving

data exchange between the EU and US. The European Court of Justice annulled the Privacy Shield in 2020 because it breached the General Data Protection Regulation.

- *2023: EU-US Data Privacy Framework*. A new framework to address previous legal objections to the Privacy Shield. Under the EU-US Data Privacy Framework businesses must meet stricter conditions regarding the security of data processing. The new rules include measures to improve transparency and strengthen controls. According to Max Schrems (the initiator of the annulments), the framework is little different from the Privacy Shield.[15]

3.5.2 The 'US access' risk in practice

On behalf of the Dutch National Cyber Security Centre (NCSC), a specialised international law firm studied the risk of American authorities using the CLOUD Act to access information stored in Europe (NCSC, 2022). 3 leading CSPs (Microsoft, IBM and Amazon) were asked how often US authorities had requested and received data on EU citizens. According to the study, these 3 providers are representative enough to draw general conclusions.

The experts at CSR and NCSC said such information was rarely requested. Amazon had never received such a request; IBM had received 1, and refused it. Microsoft had honoured 12 requests concerning users outside the United States. How many of the cases involved EU citizens, however, was not clear. The NCSC concluded from the study that the risk of the US government using the CLOUD Act to access personal data in the EU was conceivable but negligible. EU laws such as the GDPR and agreements such as the EU-US Data Privacy Framework provide some protection. Businesses can also take legal and technical measures to impede access to data, for instance through encryption.

Other routes are also available to the National Security Agency (NSA) and other US federal bodies, such as direct contact with the Netherlands General Intelligence and Security Service (AIVD).

Our audits of Microsoft and Amazon cloud services did not find that ‘personal data had been released at the request of law enforcement authorities’. It should also be borne in mind, though, that a CSP’s clients are not aware of such requests (see § 5.3).

3.5.3 Relevant EU developments

The forthcoming European Cybersecurity Certification Scheme for Cloud Services (EUCS) will provide a reference set of security requirements (assurance levels) to help member states take decisions regarding the cloud.[16] Which CSP provides what type of cloud and for what specific service? Graded certification will be introduced for certain public services and associated data sensitivities. If the EU were to insist on full application of the GDPR, EU CSPs could comply with it more easily than US CSPs because they are not subject to the US CLOUD Act.

4. Assessment of cloud policy implementation

This chapter describes the results of our audit of central government's implementation of its cloud policy and implementation framework.[17] We asked whether ministerial cloud policies and strategies, cloud oversight and risk assessments met applicable criteria.

4.1 Conclusions

Central government making avid use of the public cloud
All the ministries are using the public cloud. The main CSPs used are Microsoft, Amazon and Google. More than half of the material cloud services used by ministries are procured from these 3 US providers. Of the 1,588 cloud services used by central government, 700 (44%) are public cloud services and 477 (30%) private cloud services. The ministries do not know whether the remaining 411 (26%) are public, private or hybrid cloud.

Limited insight into cloud services
We conclude that ministries have limited insight into the cloud services they use. Only when a ministry has a proper understanding of its cloud services can it comply with applicable laws and regulations, benefit from opportunities, mitigate risks and fulfil disclosure notifications.

Two-thirds of cloud services not risk assessed
We conclude that ministries do not make enough strategic risk assessments before deciding to use a public cloud service.

Of the 700 public cloud services, 126 are classified as 'material': they are so important that their failure would prevent central government from performing its primary tasks, (e.g. collecting taxes or issuing visas). 86% of these services have not been risk assessed. There is therefore a risk that data are not adequately protected or services may be interrupted without warning. On behalf of the State Secretary for Digitalisation, moreover, CIO-Rijk cannot manage cloud risks that affect multiple ministries.

Central government expertise and purchasing power underutilised

We conclude that the ministries have little contact with the organisations responsible for strategic vendor management (SLM). They do not benefit in full from the expertise available within central government and, for example, the risk management measures included in SLM agreements with CSPs. Together, the Dutch ministries form the largest IT consuming party in the Netherlands. Using a central buyer such as SLM-Rijk could help increase coherence and consistency in the ministries' approaches to cloud services.

Differing cloud policies

We conclude that cloud policy and strategy differ from one ministry to another. The diversity makes it difficult for all stakeholders (ministries, central government data centres, cloud service providers) to make consistent agreements.

4.2 Cloud use overviews

This section looks at the results of the overviews of cloud use we requested from the ministries. Central government cloud policy requires ministries to understand what cloud services they use. We asked all the ministries to provide an overview of their cloud use in order to check their understanding. This understanding is necessary to comply with laws and regulations, make the most of the opportunities, manage risks and fulfil disclosure notifications.

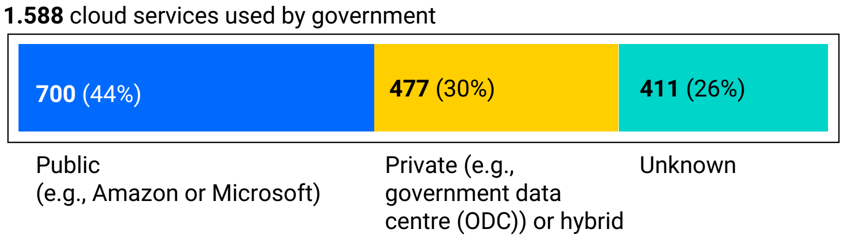
4.2.1 Total cloud use in central government

We asked the ministries to summarise their cloud use. Figure 7 shows the number of cloud services used in central government. The ministries reported 1,588 cloud services in total:

- 700 cloud services (44%) are public cloud services;
- 477 services (30%) are private or hybrid cloud services (mixed form);
- It is not known whether a significant number of cloud services, 411 (26%), are public, private or hybrid cloud.

Figure 7 *Number of cloud services reported by government, grouped by type*

Ministries do not know whether a quarter of their cloud services are hosted on a public, private or hybrid cloud



4.2.2 Insight into material public cloud use by ministry

Central government policy on cloud use applies only to material public cloud services. Of the 700 public cloud services, 126 have been designated as material. There are varying interpretations of this term among the ministries. Central government cloud policy defines material public cloud use as, *'the use of public cloud services to perform an organisation's primary task'.* A material service is therefore fundamental to the organisation.

Some ministries have adopted central government's definition; others have adapted it to their own circumstances, for instance:

- If the data processed in the cloud are sensitive, essential or difficult to replace.
- If the cloud service processes a significant proportion of the data.
- If the cloud service manages and monitors digital infrastructure and buildings.
- If the cloud service concerns interests that have to be protected in a national crisis.
- If the cloud service is necessary for essential secondary processes.
- If prolonged outage of a cloud service would have serious consequences for citizens.
- If data falling into the hands of third parties would have serious consequences.

The ministries' differing definitions lead to differences in their approach to material public cloud services. The approach begins with monitoring the services but, more importantly, managing the risks. As noted above, central government cloud policy applies only to material public clouds. Its risk assessment, data protection and other policy conditions do not apply to non-material applications. Differences in the ministries' reports to CIO-Rijk also paint an incomplete picture because some of the risks remain underexposed.

Given the differing interpretations of material public cloud use, we asked the ministries to prepare comprehensive overviews of both their public, private and hybrid cloud use and their material and non-material use.[18] We used this information to assess whether the ministries had an understanding of all their cloud usage. The same overviews were used to assess whether the ministries had an insight into their reported material public cloud services. Table 1 shows whether or not ministries had an insight into whether their reported cloud services were material and whether they used a public, private or hybrid cloud.

As noted in § 2.3, some ministries rely on other ministries for data processing. The Minister of A&M, for instance, relies on the Ministry of J&V. The Ministry of VRO relies on the Ministry of BZK and the Ministries of KGG and LVVN on the Ministry of EZ. More than one minister is responsible for these ministries. Our findings relate to the 11 ministries shown in the tables in this chapter.

Table 1 *Insight into material public cloud by ministry*

	AZ	BZ	BZK	DEF	EZ	FIN	I&W	J&V	OCW	SZW	VWS
Insight into material public cloud	✓	✓	✓	✓	✗	✗	~	✓	✗	~	~

Meets the criterion
✓ yes ~ partially ✗ no

Some ministries improved their insight into cloud services in six months

Central government introduced its cloud policy in September 2022. Ministries needed time to implement it. We took this into account in our audit and investigated the situation at all ministries in autumn 2023 and again in mid-2024. In the intervening period some ministries, e.g. BZ, BZK, Defence and J&V, improved their insight into their cloud use.

4.2.3 Insight into characteristics of material public cloud by ministry

Central government cloud policy requires ministries to keep a record of at least the following characteristics of the material public cloud services they use:

- Organisational unit,
- Business process,
- Supplier,
- Risk assessment performed.

We analysed the ministries’ overviews of their material public cloud services to check whether these characteristics were known. Our findings are presented in table 2

Table 2 *Insight into characteristics of material public cloud services by ministry*

	AZ	BZ	BZK	DEF	EZ	FIN	I&W	J&V	OCW	SZW	VWS
For the material public cloud services, does the ministry have an insight into the *relevant organisational entity, business process, supplier and risk assessment characteristics?*	✓	✓	✓	✓	~	✓	✓	~	~	✓	~

Meets the criterion

✓ yes ~ partially ✗ no

Of the 11 ministries, 7 self-reported that they knew the organisational unit, business process and supplier of their material public cloud services and whether a risk assessment had been made. Their overviews also revealed that more than half of the material public cloud services were procured from 3 major US providers (Microsoft, Amazon and Google). We did not verify the information provided by the ministries regarding the organisational unit, business process or supplier. We did check the information they provided on whether a risk assessment had been performed, as explained in the section § 4.3 below.

Besides the 4 characteristics we analysed, we asked about the geographical location and the contractual start and end dates. Many of the overviews of cloud usage we received did not include the start and end dates. In some cases, moreover, the identity of the cloud service provider was not known. It was not always known what data were processed in the cloud and in many cases the geographical location of the cloud service was not known. These characteristic are not required under central government cloud policy but they shed a light on the ministries’ management of their cloud use.

Ministries therefore have limited insight into what data are stored and processed by which CSP and in what geographical locations. This is an additional risk exposure if data are processed in countries with potentially hostile state actors and amenable laws. Safe use of the cloud requires an understanding of the CSP chain and its security measures.[19] We consider these aspects in more depth in our assessment of 3 material public cloud contracts in chapter 5.

> **Good example of ministry insight: the Ministry of BZK**
>
> The Ministry of BZK began keeping a cloud register in 2022, before we began our audit. Its overview of cloud use was based on an earlier internal analysis. It covered 156 cloud services, 12 of which were classified as material public cloud services. The ministry knew the organisational unit, business process and supplier of each material public cloud service. It also knew nearly all the other characteristics, such as contract dates and geographical location. The Ministers of BZK and VRO therefore have a good insight into the cloud services they use.

4.3 Risk assessment method

4.3.1 Risk assessment method and performance

This section presents our findings on the risk assessment of material public cloud use. If a central government organisation needs a new system for its customer contact centre, for instance, it can choose an inhouse system or a cloud-based system. In both cases, it must assess the opportunities and risks (see § 3.3 and elsewhere in this report).

Under central government cloud policy, ministries must have and apply a risk assessment method. In our opinion, risk assessments should be systematic. We therefore investigated whether the ministries had a risk assessment method,[20] and then checked whether it had been applied to material public cloud contracts. If risks are not assessed in accordance with the method, they should be assessed in another way. Table 3 presents our findings by ministry.

Table 3 *Risk assessment of material public cloud services by ministry*

	AZ	BZ	BZK	DEF	EZ	FIN	I&W	J&V	OCW	SZW	VWS
Method present	✓	✓	~	✓	✓	✓	✗	✓	✓	✓	✓
Method formalised	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓
Risk assessment performed (using a risk assessment method or otherwise)	~	~	~	~	~	~	~	~	~	✓	~

Meets the criteria

✓ yes ~ partially ✗ no

Nearly all ministries had assessed the risks of only some material public cloud contracts before taking the service into use. Across central government, risk assessment documents were available on only 42 of the 126 material public cloud contracts. Risk assessments had therefore not been made of two-thirds of the material public cloud contracts. Only the Ministry of SZW had assessed the risks of all its material public cloud contracts, as should be expected.

Piecemeal risk assessments after 6 months

As noted above in this chapter, we investigated the situation at the ministries in late 2023 and mid-2024. We received only a few additional risk assessments in that half year, despite the assessment method being introduced and formalised more widely at many ministries. Applying it improved the assessment of cloud-related risks

As the ministries do not make comprehensive risk assessments, they have only a limited understanding of the risks. If risks are not known, they cannot be mitigated and the risks will persist. Data will not be protected effectively and service delivery may be unintentionally disrupted. Insight into risks at central government level, too, is limited. The State Secretary for Digitalisation accordingly cannot manage, via CIO-Rijk, interministerial risks of material public cloud services.

4.3.2 Consultation with strategic vendor management organisations

Central government cloud policy requires ministries to consult strategic vendor management (SLM) organisations in order to re-use previous analyses and, where possible, take joint action. In other words, they can refer to SLM's risk assessments and other analyses it has already carried out. If it is known that a ministry intends to use a particular cloud service it can be procured jointly with other ministries.

Table 4 *Consultation with strategic vendor management (SLM)*

	AZ	BZ	BZK	DEF	EZ	FIN	I&W	J&V	OCW	SZW	VWS
Consultation with strategic vendor management (SLM)	✗	✗	✗	●	✗	✗	~	✗	~	✗	✗

Meets the criterion

✓ yes ~ partially ✗ no ● not applicable

Only 2 ministries said they had consulted an SLM organisation with regard to their material public cloud services, and had done so for only some of their contracts. The other ministries had not explicitly consulted SLM for any of their cloud contracts.

We learnt from SLM that ministries sometimes contracted cloud services subject to master agreements that SLM had concluded with cloud service providers, such as Microsoft, without consulting it. Not all ministries and their agencies use such master agreements, possibly because the contract with a public CSP is concluded through an intermediary that has a contract with the ministry. Contracts could also have been concluded before a master agreement became available. Failure to use a master agreement can lead to higher costs and non-compliance with central government agreements.

4.3.3 Cost-benefit analyses

In addition to implementing central government cloud policy, the costs and benefits of using a public cloud should be assessed. As noted in § 3.3.1, the cloud has the potential to save costs. Central government should carefully analyse both the short and the long-term financial aspects and different cost structures (purchase/licence) of cloud use. Poor financial analysis can lead to inadequate financial cover and jeopardise business continuity.

Table 5 *Cost-benefit analyses*

	AZ	BZ	BZK	DEF	EZ	FIN	IenW	J&V	OCW	SZW	VWS
Costs and benefits assessed	~	✗	✗	~	✗	✗	✗	✗	✗	✗	✗

Meets the criterion
✓ yes ~ partially ✗ no

Barely any of the ministries had made cost-benefit analyses. Table 5 shows that only AZ and Defence had analysed some of the financial aspects of their material public cloud contracts.

4.4 Policy and strategy

The implementation framework for central government cloud policy states that *'All units of a public service formulate their own cloud policy and strategy subject to the frameworks of central government cloud policy and this implementation framework'*. Without a cloud policy and strategy, ministries will take ad hoc decisions that might not be consistent with central government policy and the implementation framework. Central government cloud policy must be tailored to each ministry and agency's circumstances.

We checked whether the ministries had formulated and formalised a strategy and policy and whether they incorporated central government cloud policy. Our findings are presented in table 6.

Table 6 *Ministerial policy and strategy*

Ministerial policy and strategy	AZ	BZ	BZK	DEF	EZ	FIN	I&W	J&V	OCW	SZW	VWS
Present	✓	✓	✓	✓	~	✓	~	✓	~	✓	✓
Formalised	✓	✓	✓	✓	✓	~	✓	✓	✓	✓	✓
Formalised strategy or policy incorporates the central government cloud policy	✓	✗	✗	●	✗	~	✓	✓	✓	✓	✓

Meets the criteria
✓ yes ~ partially ✗ no ● not applicable

8 of the 11 ministries have a cloud policy and strategy. The remaining 3 have either a policy or a strategy but not both. Most ministries have also formalised the policy or strategy. The Ministry of Finance has formalised the policy but not the strategy (a strategy was prepared in mid-2024). Only 6 of the 11 ministries have incorporated central government cloud policy into their own policy or strategy. One reason given for not incorporating it is that the ministerial cloud policy had been formalised before the new central government cloud policy was introduced. This, for instance, was the case at the Ministry of BZK. We did not check whether ministerial cloud policies were consistent with the central government cloud policy.

Good example of a ministerial cloud policy: the Ministry of Defence

The Minister of Defence sets a good example of what a cloud strategy should embody. Its strategy includes requirements, opportunities and risks, the cloud ambition, strategic choices and assessment criteria, frameworks, action lines and relevant developments in central government. It explains that the traditional approach to secure IT in the ministry’s own data centres is no longer appropriate given the current state of the market in general and the IT sector in particular. To make the most of technical innovations, the ministry is gradually working towards a hybrid IT landscape that accommodates both private and the public clouds. The ministry also stresses that a movement towards the cloud is necessary to support the defence organisation’s tasks, especially in the light of geopolitical developments. Modern technology and conventional force are closely related to each other in a military conflict. The cloud is undergoing rapid change. To keep pace, the Minister of Defence has prepared several policy documents and an assessment framework in recent years.

Several ministries made good progress with their cloud policies and strategies during our audit. In autumn 2023, for instance, the Ministry of SZW had neither a cloud policy nor a strategy. By mid-2024 it had formalised both a policy and a strategy that incorporated central government policy. The Ministry of J&V has recently also formalised a new cloud strategy.

We found that cloud strategies and cloud policies differed from one ministry to another, not only regarding the concept of materiality discussed in § 4.2.2. The differences make it difficult for all involved (ministries, government data centres, CSPs) to make consistent agreements. This may also be true of the base registries that central government uses to work with local authorities.

4.5 Role of the State Secretary for Digitalisation

On behalf of the State Secretary for Digitalisation, CIO-Rijk monitors the implementation of central government cloud policy and reports to the House of Representatives. This is generally going well. Via CIO-Rijk, the state secretary can better control the information provided by the ministries. The information they provide to CIO-Rijk differs significantly in amount and detail. This makes it of little use to gain a full understanding of the ministries' implementation of central government cloud policy. Our audit found that, on behalf of the State Secretary for Digitalisation, CIO-Rijk does not reproach ministries that do not fully answer questions about their cloud policy and cloud use in relation to central government cloud policy.

The State Secretary for Digitalisation asked the Central Government Audit Service (ADR) to carry out an audit of the cloud (ADR, 2024). The audit investigated the monitoring of the implementation of central government cloud policy. The ADR audited 3 public cloud services that were used in central government and that ministers volunteered for this audit in consultation with CIO-Rijk. In brief, implementation of central government policy is a work in progress.

The State Secretary for Digitalisation provides the House of Representatives with periodic updates of central government cloud policy (BZK 2023d, 2024a and 2024b). The letters also include a summary of the progress made with parliamentary motions concerning the cloud. Officials from CIO-Rijk also give technical briefings to the House.[21] A recent letter from the state secretary to the House specifically considered an evaluation of central government cloud policy (BZK, 2024c). The letter's main findings are consistent with our findings and conclusions.

5. Contractual safeguards of the 3 principes

We audited 3 important public cloud contracts. This chapter presents our conclusions and findings. We expect the ministers concerned to have an insight into their contractual agreements and to protect digital sovereignty, business continuity and data confidentiality. We asked the ministries to demonstrate that these 3 principles were contractually safeguarded. We also asked them to verify that the agreements with CSPs were adhered to in practice. Using this information, we can present a picture of how ministers draw up public cloud contracts and how CSPs adhere to them. Our findings cannot be generalised and applied across all of central government, but they do give an impression of the safeguards in place for digital sovereignty, business continuity and data protection.

5.1 Conclusions

We investigated 3 material public cloud contracts that were substantial in size and related to important public services. They concerned:

- Microsoft 365 at the Shared Service Centre-ICT (SSC-ICT),
- Systems at the Royal Netherlands Meteorological Institute (KNMI),
- CIBG's customer contact centre.[22].

Inadequate measures to safeguard digital sovereignty, business continuity and data protection.
We conclude that the ministries concerned have not taken sufficient measures to safeguard digital sovereignty, business continuity and data protection in public cloud contracts. This means central government will be exposed to risks if, for instance, a CSP is hacked.

Central government will then no longer be able to deliver goods and services to citizens and businesses. There is also a risk of personal and commercial data being inadequately protected and misused by malicious and state actors.

Weak grip on contractual agreements for public cloud services

We conclude that the ministries' grip on contractual agreements for public cloud services is weak. There is no comprehensive overview of or insight into all contractual agreements. Several parties are often involved in providing a public cloud service, including shared service organisations (SSOs) and subcontractors. We found that contractual arrangements were complicated and laid down in multiple agreements. The ministries have only limited knowledge of the agreements. This is problematic because the purpose of contractual agreements is to mitigate risk.

The risks to the 3 principles of digital sovereignty, business continuity and data protection are discussed below.

Digital sovereignty

Where a ministry delegates tasks and responsibilities to a third party (such as a CSP), there is a risk of it having too little influence over decisions taken on:

- the design and use of business processes that use the ministry's own data;
- who has access to the ministry's data;
- how the ministry's data are processed by the CSP.

The ministry is thus possibly unable to comply with applicable European and national laws and regulations, such as the GDPR. This is illustrated by the example given in § 2.1.2, in which a Chinese hacker used a Microsoft engineer's device to access emails at the US Department of State.[23]

Business continuity

The ministry's great reliance on a third party (the CSP) and the absence of a plan B put it at risk of being unable to deliver goods and services to citizens and businesses. An example of this already mentioned is the threat to Atos's future as a going concern. Atos is an IT provider that plays an important role in several vital central government processes.[24]

Data protection

As the ministry's data are stored, processed and transmitted in the cloud, there is a risk of personal and commercial data being inadequately protected and misused by malicious actors. Examples mentioned above include the stolen contact data of all police personnel in the Netherlands and the hacked US Department of State's emails.[25]

Below, we provide a further description of the contracts we audited and then present our findings on each of the 3 principles.

5.2 The contracts and cloud provider chain

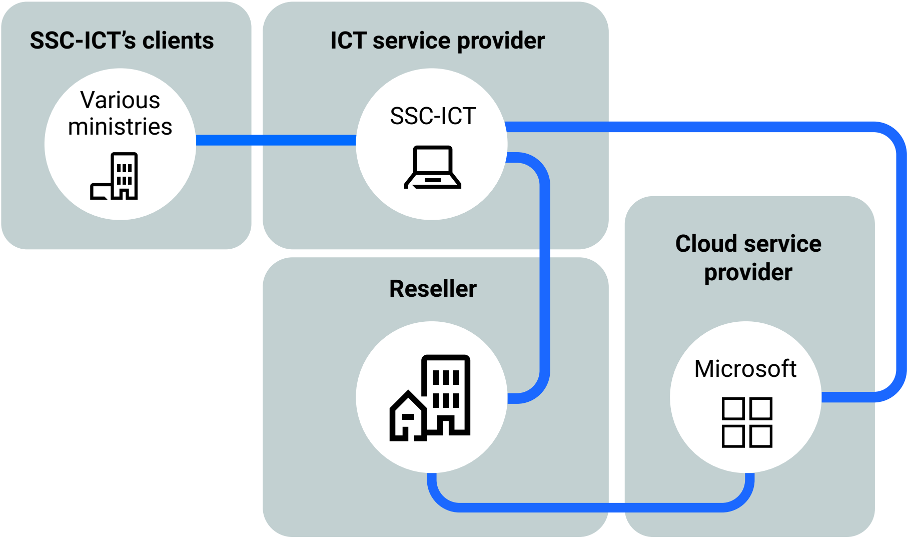
5.2.1 The cloud service provider chain

From the ministries' summaries (see § 4.2), we selected 3 important material public cloud contracts for our audit.[26] The contracts concerned the delivery of public services to citizens and businesses. We first took a close look at the CSP chain as it is a significant factor in all 3 contracts.

IT landscapes are often complex. It is rarely the case that a ministry concludes a contract directly with a CSP. Many cloud contracts are concluded jointly with other ministries through a shared service organisation (SSO). The SSO itself often concludes the contract with a reseller rather than directly with the cloud provider. Figure 8 shows the CSP chain for Microsoft 365 at SSC-ICT. The ministries themselves do not conclude a contract with Microsoft but select the service from SSC-ICT's products and services catalogue. Microsoft has authorised a reseller to sell Microsoft licences.

Figure 8 *A cloud service provider chain*

The supply chain is complex



5.2.2 SSC-ICT's contract for M365

At the Ministry of BZK, SSC-ICT has signed a contract with Microsoft for the M365 Cloud Development Environment. Under the contract, SSC-ICT has established a central government work environment / digital work environment for its clients. Since 1 May 2024, the contract has applied to SSC-ICT itself and to all users of its central government work environment (about 40 in total). SSC-ICT has concluded a contract with both Microsoft and a reseller, as shown in figure 8.

The services provided by SSC-ICT: SSC-ICT describes itself on its website as follows, *'We are SSC-ICT, one of the biggest ICT service providers of and for central government. With our ICT services, we ensure that more than 57,000 civil servants at 7 ministries can always carry out their work safely at the service of society as a whole.'*[27]

About Microsoft 365: Microsoft 365 is a suite of internet services similar to the Microsoft Office package (including word processing, spreadsheets, and an email programme). Instead of installing the software on computers owned by an organisation or on its premises, Microsoft 365 runs on servers installed and managed by Microsoft. Microsoft 365 is accordingly an online public cloud service available on every platform that supports the internet.

5.2.3 CCIBG's contract for KLOPT

At the Ministry of VWS, CIBG28 (Central Information Point for Healthcare Professions) uses KLOPT for its customer contact system. The service is provided through a main contractor and a subcontractor and is procured from Amazon Web Services (AWS).

The services provided by CIBG: CIBG is an agency of the Ministry of VWS. Its website presents a selection of its tasks and activities.29

- We register healthcare providers, veterinarians, people's choices about organ donation, people with a Social Hygiene diploma.
- We publish annual reports of healthcare institutions.
- We test top incomes in healthcare, new healthcare institutions.
- We set maximum prices for medicines.
- We produce medicinal cannabis or have it produced.
- We recognise tissue banks and blood banks, foreign diplomas for professions in the healthcare sector.
- We provide access passes to healthcare providers for access to digital patient data and secure email messaging, drug licences, donor test lab licences, opium exemptions.

About KLOPT: The CIBG uses the KLOPT customer optimisation application for its customer contact centre (KCC) The KCC is CIBG's central helpdesk to answer questions from its clients (citizens, businesses, professionals and organisations). The questions are received and answered through a variety of channels (including by telephone, mail, in person and by letter). The KCC receives clients' questions, reports and complaints regarding a variety of products, such as the donor register and CIBG's services in general. It then enters the information in KLOPT for processing, where necessary with support from its back office staff and Legal Affairs department. CIBG has signed a contract with a main contractor that works with a subcontractor to provide telephony services and the KCC application on AWS's cloud platform.

5.2.4 KNMI's contract for AWS's core cloud platform

At the Ministry of I&W, the Royal Netherlands Meteorological Institute (KNMI) uses the Amazon AWS Cloud as its core cloud platform. The contract was concluded through SURF, the ICT cooperative of Dutch education and research institutions. The following box contains more information on SURF.

The services provided by KNMI: KNMI's website includes the following description of its services: *'The Royal Netherlands Meteorological Institute (KNMI) is the Dutch national weather service. Primary tasks of KNMI are weather forecasting and monitoring of weather, climate, air quality and seismic activity. KNMI is also the national research and information centre for meteorology, climate, air quality, and seismology.'*

About Amazon AWS Cloud: In the information it provided, KNMI describes the platform as, *'the core cloud platform with many operational applications, from observations to services for the outside world'*.

Good example of cooperation: KNMI and SURF

SURF is the ICT cooperative of Dutch education and research institutions. Established in 1986, its members decide whether, how and through which service provider they use cloud services. Our audit of the contract analysed the cloud service chain. The end user (in this case KNMI) can decide which cloud service it wishes to buy from SURF. SURF provides the service. KNMI can also contact AWS directly. The move to public cloud services is better controlled if central government entities combine their strengths.

5.3 Outcome of our audit of 3 public cloud contracts

Our audit of 3 important cloud contracts found that central government is exposed to risks regarding digital sovereignty, business continuity and data protection. The organisations we audited paid inappropriate attention to risk management.

We found that contractual arrangements were complicated and laid down in several agreements. The ministries have only limited knowledge of the agreements. There is no comprehensive overview of or insight into all contractual agreements. This is problematic because the contracts are intended to mitigate risk.

Table 7 presents all the outcomes of our tests of whether the 3 contracts met the criteria set for the 3 principles. The criteria are detailed in appendix 2. The paragraphs following the table below explain the criteria and the findings on each of the 3 principles, with a good example of the principle in a text box.

Table 7 *Audit findings on 3 public cloud contracts*

Criteria no.	Subject	BZK - SSC-ICT		VWS - CIBG		I&W - KNMI	
		Design	Implementation	Design	Implementation	Design	Implementation
	Sovereignty						
S1	Risk assessent & contract agreements	~	~	✓	✓	✗	✗
S2	Interoperability & portability - roles and responsibilities	~	✗	~	✗	✓	✗
S3	Interoperability & portability - contract termination	~	✗	~	✗	~	✗
S4	Interoperability & portability - transferability	✗	✗	✗	✗	~	✗
S5	Disclosure notification	✓	●	✗	✗	✓	●
S6	Data flows and location	~	✓	✓	✓	~	✓
S7	Right to audit	✓	✓	~	~	~	●
	Business continuity						
C1	Continuity of operations	~	~	✗	✗	✗	✗
C2	Backup and data replication	✓	✗	~	✗	~	✗
C3	Change management	✓	✓	~	~	~	✗
C4	Security incidents	✓	●	~	~	~	~
	Data protection						
G1	Governance	~	✓	~	✗	~	✗
G2	Encryption	~	~	✓	✓	~	✗
G3	Access control	✓	~	~	✗	✓	✗
G4	Supply chain	✗	✗	✗	✗	✗	✗
G5	Vulnerabilities	✗	✗	✓	~	~	✗
G6	Infrastructure security	✗	✓	✓	✓	✓	✓

Meets the criteria ✓ yes ~ partially ✗ no ● not present

Design: 'on paper' - whether the measures are laid down in contracts, agreements, processes or procedures.
Implementation: 'in practice' - whether the measures are demonstrably present in practice.

5.3.1 Digital sovereignty

Our audit included an analysis of whether the ministries carried out risk assessments before concluding contracts. Risk assessments enable them to identify, discuss and mitigate potential cloud risks. We also checked whether the ministries took measures to enable the transfer of data to another cloud provider. This is particularly important if a ministry wants to switch to a different CSP, for instance in an emergency or if the CSP is hacked.

The cloud infrastructure must work smoothly with a ministry's other systems. We therefore checked whether the ministries took measures to enable interoperability, such as data-sharing between systems.

Some state actors can ask cloud service providers to provide them with the personal data they process or store for their clients. We therefore checked whether the ministries took measures to ensure that requests by law enforcement authorities to release personal data complied with applicable laws and regulations.

A ministry should be informed by an independent party – such as an auditor – whether the cloud provider adheres to its agreements. We checked whether the ministries negotiated the right to audit the cloud provider. The auditor could be, but not necessarily so, the Court of Audit.

Good example of risk assessment on conclusion of a contract: CIBG

CIBG is an executive agency of the Ministry of VWS. It correctly assessed the risks before concluding its contract with AWS. The risk assessment procedure began with the call for tenders. Tenderers were asked to explain how they would mitigate specific cloud risks, such as the misuse of data or a configuration error in the shared cloud environment. During the tendering process, CIBG carried out due diligence, with an emphasis on security measures. It verified the implementation of the security measures during an on-site visit. It also carried out pentests to detect vulnerabilities. The vulnerabilities were recorded in a Risk Acceptance Document (RAD) and accepted by CIBG's directors. The Minister of VWS is responsible for CIBG.

Findings

Our audit found that the 3 contracts do not effectively manage the risks that arise on the termination of a cloud contract. Contractual agreements on the retention or transfer of data to other systems were also inadequate.[30] Central government is therefore exposed to risks, for instance if the cloud provider is hacked. That this is a realistic risk is demonstrated by recent reports on the threat to Atos's future as a going concern. Atos is an important provider of IT services to central government.[31] Our audit further found that roles and responsibilities were not clearly allocated to the ministries and cloud providers.

5.3.2 Business continuity

We investigated, among other things, whether the ministries had taken contingency measures to ensure they could continue to deliver critical services in a crisis. We also checked whether the contingency plans agreed with the cloud provider were tested in practice.

Unannounced changes in the cloud infrastructure can interrupt the ministry's service delivery. We therefore investigated whether the ministry and the cloud provider had made clear agreements on change processes and whether the agreements were observed in practice.

If the CSP and a ministry have not made clear agreements on the reporting of security incidents, neither party can respond appropriately. This can compromise the ministry's service delivery. We therefore investigated whether clear agreements had been made to report security incidents.

Good example of change management and response to security incidents: SSC-ICT

SSC-ICT is an executive organisation of the Ministry of BZK. It has included robust provisions on change management and security incidents in its contract with Microsoft. The contractual provisions explain how Microsoft will inform its client (SSC-ICT) of significant changes and of the client's responsibilities. There are also provisions on how Microsoft will respond to security incidents and on each party's responsibilities. The Minister of BZK is responsible for change management and responding to security incidents. In our opinion, these aspects of the contract with Microsoft are in order.

Findings

Our audit found that business continuity is only partially safeguarded. SSC-ICT has put the most safeguards in place for KNMI and CIBG. None of the 3 cloud contracts we audited contained clear safeguards on business continuity. We expect cloud contracts to include contingency planning arrangements. We also expect agreements to have been made on the resumption of a ministry's service delivery from a different location if one of the CSP's locations is no longer available.

5.3.3 Data protection

We investigated whether the ministries and their CSPs made clear agreements on their data management roles and responsibilities. Vague agreements can lead to failure to take the security measures necessary to protect data on a ministry and the citizens and businesses it serves.

Unauthorised data access can lead to the theft, corruption or deletion of a ministry's data. We therefore checked whether the ministries and cloud providers had made agreements on data access. We further checked whether the CSPs acted appropriately to prevent access to the ministries' data by other consumers of the cloud.

Good example of IT infrastructure security: CIBG

The Minister of VWS has included measures in its contract with AWS to secure CIGB's IT infrastructure effectively. The cloud application runs on a shared physical IT infrastructure. One of the contract award criteria was that data had to be isolated from other consumers on the same cloud. Data had to be available exclusively to the owner and not to any other consumer. CIBG visited the location to verify that this was the case.

Findings

Our audit found that the safeguards in place for data protection were inadequate. None of the CSP chains in the 3 contracts had effective data protection measures. Weak access control also increased the risk of unauthorised staff members accessing data.

6. Conclusions and recommendations

This chapter presents our main audit conclusions and recommendations.

6.1 Conclusions

Our audit findings lead us to the following conclusions:

Opportunities and risks
Cloud computing is an opportunity for central government to save costs and increase its efficiency, availability and accessibility, security and privacy, and innovation capacity. However, there are also risks to digital sovereignty, business continuity and data protection.

Conclusions on the audit of central government cloud use
We audited the insight into cloud use, risk assessment and policy and strategy at all the ministries.

Central government making avid use of the public cloud
All the ministries are using public clouds. More than half their material public cloud services are procured from 3 American companies: Microsoft, Amazon and Google. Of the 1,588 cloud services used in central government, 700 (44%) are public cloud and 477 (30%) private or hybrid (i.e. mixed) cloud. The ministries do not know if 411 (26%) of their cloud services are public, private or hybrid.

Insight into cloud services
We conclude that ministries have limited insight into the cloud services they use. If a ministry has a proper understanding of its cloud services, it is in a better position to comply with applicable laws and regulations, maximise opportunities, mitigate risks and fulfil disclosure notifications.

Risks of two-thirds of cloud services not assessed
We conclude that ministries do not perform appropriate strategic risk assessments before deciding to use a public cloud. Of the 700 public cloud services, 126 are material (i.e. used to perform the organisation’s primary task, such as collecting taxes or issuing visas). The risks of 84 (67%) of the services have not been assessed. There is therefore a risk of data not being protected or services being interrupted without warning. CIO-Rijk cannot effectively manage interministerial cloud risks on behalf of the State Secretary for Digitalisation.

Central government expertise and purchasing power not fully utilised
We conclude that the ministries have little contact with strategic vendor management (SLM) organisations and accordingly do not benefit in full from central government expertise and, for example, the risk mitigation measures in SLM agreements with cloud providers. Together, the Dutch ministries form the largest IT consuming party in the Netherlands. Using a central buyer such as SLM-Rijk can help increase coherence and consistency in the ministries’ approaches to cloud services.

Differing cloud policies
We conclude that cloud strategies and policies differ from one ministry to another. The diversity makes it difficult for stakeholders (ministries, central government data centres, cloud providers) to make consistent agreements.

Conclusions on the 3 material public cloud contracts audited
We audited 3 material public cloud contracts. They were substantial contracts for important public services:

- Microsoft 365 at the Shared Service Centre-ICT (SSC-ICT),
- systems at the Royal Netherlands Meteorological Institute (KNMI)
- the customer contact centre at CIBG.[32].

Weak measures to safeguard digital sovereignty, business continuity and data protection
We conclude that the ministries take inadequate measures in public cloud contracts to safeguard digital sovereignty, business continuity and data protection. Central government is therefore exposed to risks. For example, if a cloud provider is hacked, the government might be unable to deliver goods and services to citizens and businesses. There is also a risk of personal and commercial data not being adequately protected and being misused by malicious and state actors.

Weak control of contractual agreements for public cloud services
We conclude that the ministries exercise too little control over their contractual agreements for public cloud services. There is no comprehensive oversight of or insight into all contractual agreements. Several parties are often involved in a public cloud service, for example shared service organisations (SSOs) and subcontractors. We found that contractual arrangements were complex and were laid down in multiple agreements. The ministries have only limited knowledge of the agreements. This is problematic because contractual agreements are intended to mitigate risk.

Main conclusions and opinion

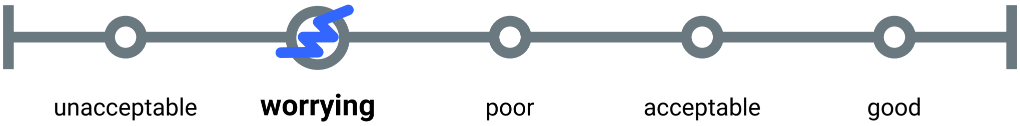
For this audit we examined ministries' compliance with central government cloud policy and asked whether the principles of digital sovereignty, business continuity and data protection were safeguarded. We draw the following conclusions:
Central government has limited insight into its cloud services.

1. Central government makes insufficient strategic risk assessments.
2. Central government inadequately safeguards the principles of digital sovereignty, business continuity and data protection in the 3 public cloud contracts we audited.
3. We conclude from our audit that central government is making ill-considered use of the cloud and has too little control over its cloud use.

Our audits of policy outcomes include an opinion based on a 5-point scale: unacceptable, worrying, poor, acceptable, good.

In our opinion, central government's use of the cloud is worrying. The continuity of public services is exposed to too much risk. The potential damage caused by an interruption of public services could disrupt our country and society. Cloud policy and its implementation, moreover, cannot be seen in isolation from current geopolitical uncertainties.

Overall opinion



We would note that during the audit period several ministers made progress in various areas, including improving their insight into cloud services and adopting ministerial policies. In other areas (risk assessment, contractual provisions to safeguard principles), however, substantial improvements are still needed.

6.2 Recommendations

Our main recommendation, to all ministers:
To safeguard digital sovereignty, business continuity and data protection, central government should act as a unified organisation and set frameworks, enforce rules, mitigate risks and strengthen its relationship with the major cloud service providers and other cloud users. To do so, it needs a better insight into its own cloud use and assess opportunities, risks and alternatives in greater detail both before and also during its use of the cloud.

We elaborate on this main recommendation in the secondary recommendations and explanatory notes below.

To the Minister of BZK:

Recommendation 1
Make cloud policy more uniform and specific and oversee its implementation:

- More uniform: by permitting the fewest possible departures in ministerial policy and, for instance, by making the guidelines on risk management and use of the public cloud obligatory. Explore the possibilities of extending central government cloud policy to local authorities and autonomous administrative authorities (ZBOs).
- More specific: by, for example, specifically stating that certain public services may never be hosted on a public cloud.

Explanatory note: our audit found that central government organisations worked differently with the cloud. We saw that the differences had a negative impact on risk management. Moreover, central government cloud policy has only limited scope within the public sector because it does not apply to ZBOs and local authorities. The entire public sector is exposed to risks. A well-known example of central government policy that applies to all central government organisations is the Information Security Baseline (BIO). The cloud is a key factor in digital security, and therefore requires a central government policy.

Recommendation 2
Strengthen the enforcement of central government cloud policy. Compliance with central government cloud policy is currently too discretionary. Through CIO-Rijk, the State Secretary for Digitalisation should enforce the policy more proactively in close collaboration with the ministerial CIOs and with procurement officers and other experts.

Recommendation 3
Have all ministers improve their insight into the cloud services they use and assess the risks of material public cloud services that have not yet been risk assessed.

Explanatory note: our audit revealed that the ministries' compliance with the conditions in central government cloud policy (e.g. risk assessment) is limited. In addition, there are significant differences in the amount and detail of the information on the cloud that they provide to CIO-Rijk. The cloud is usually a matter for the chief information security officer (CISO), but it should be approached from a variety of angles, including strategic procurement, vendor management and privacy. The State Secretary for Digitalisation should have CIO-Rijk take more account of these specialisations and work with them.

To all ministers:

Recommendation 1
Central government should focus more on joint procurement, the negotiation of favourable conditions and the performance of audits. A central strategic vendor management (SLM) organisation could take the lead to make the conclusion of cloud contracts more efficient. In an EU context, there are opportunities for central government to collaborate on the standardisation, certification and enforcement of GDPR provisions. Central government should study realistic EU alternatives in combination with a practical exit strategy.

Explanatory note: if every ministry opts for the easiest and least expensive solution, central government will become ever more reliant on a handful of dominant cloud service providers. It should therefore act more as a unified body with regard to procurement, enforcement of conditions (e.g., GDPR provisions) and risk management. It should then satisfy itself, for instance by means of joint audits, that cloud providers meet its conditions.

Central government should act more as a unified organisation when dealing with the major cloud providers and make use of at least the framework agreements made by the various departments within central government that are responsible for strategic vendor management (SLM). Together, the Dutch ministries form the largest IT consuming party in the Netherlands. Using a central buyer such as SLM-Rijk could help increase coherence and consistency in the ministries' approaches to cloud services. As noted in § 2.2.1, SLM is fragmented. It would be more logical to have a central SLM organisation for IT services, not least in order to compare different cloud services and negotiate generic conditions.

Discussions of the cloud sometimes assume that only US and Chinese companies provide cloud services. However, there are also European initiatives, as mentioned in this report. The EU could promote standardisation and certification and thus act as a platform for common substantive requirements. The proposal for a European Cybersecurity Certification System is a first step in this direction, see also § 3.5.3.

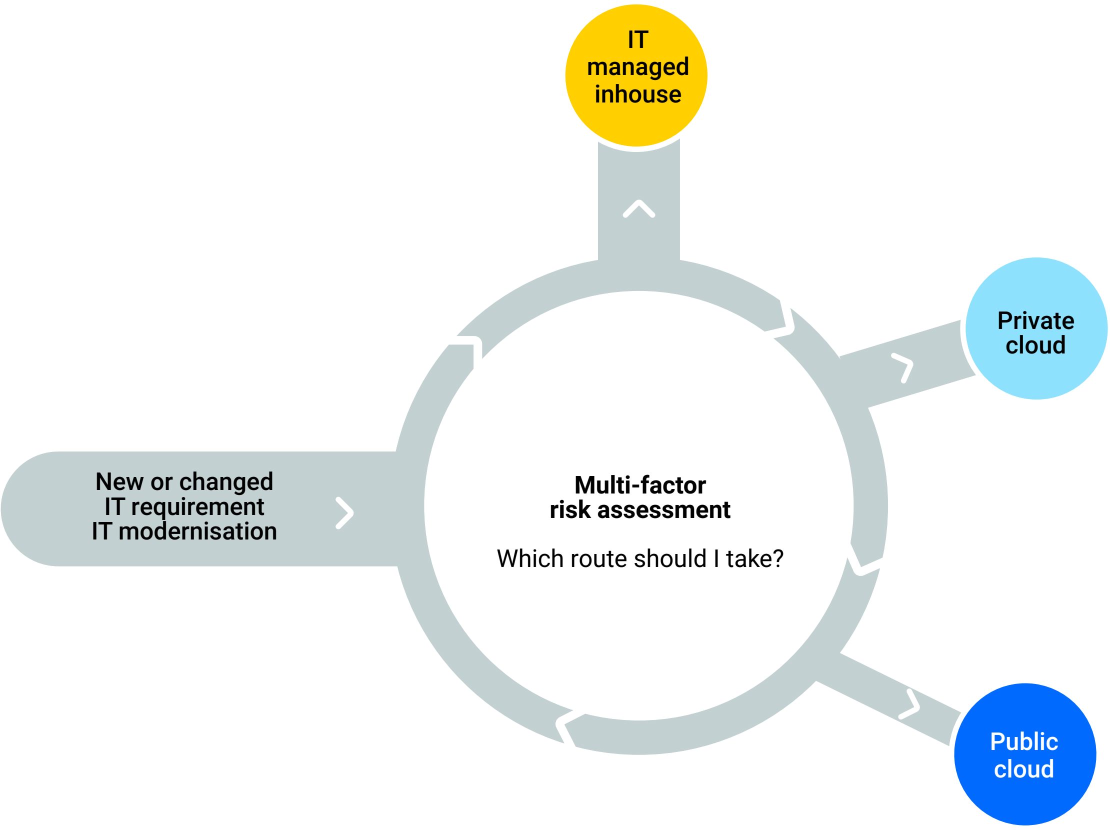
Recommendation 2
Assess the risks of every new cloud service that is proposed and update risk assessments of cloud services already under contract. Opportunities and risks can differ from one cloud to another. The assessment should in any event consider the principles of digital sovereignty, business continuity and data protection. Other aspects, such as cost, innovation capacity and requisite knowhow and skills, should also be considered.

Recommendation 3
Improve insight into the cloud services already in use and assess the risks of material public cloud services that have not yet been risk assessed. Take risk mitigation measures, for instance by agreeing additional contractual provisions and verifying compliance with them.

Explanatory note: the IT landscape should be the product of careful decisions. What can be placed in the cloud and what cannot, and which type of cloud is the most appropriate? The opportunities and risks of each cloud service can differ. It is crucial that they are assessed. This is illustrated in figure 9. It is relevant to new cloud services and to cloud services that are already in use but have not yet been risk assessed. The risks are simply too high, as outlined in this report.

Figure 9 *Multifactor risk assessment of IT environment*

Central government must improve its risk assessment to choose the most appropriate location of IT sourcing


IT managed inhouse
Private cloud
New or changed IT requirement IT modernisation
Multi-factor risk assessment
Which route should I take?
Public cloud

7.
Response and afterword

We received the State Secretary for Digitalisation's response to our draft report on 9 December 2024. We reproduce the most relevant part below. The state secretary's full response can be found (in Dutch) at rekenkamer.nl. We close this chapter with our afterword.

7.1 Response of the State Secretary for Digitalisation

The State Secretary for Digitalisation thanks us for the report. It provides important insights, he writes, into central government's use of the public cloud and where improvements can be made. He further writes:

'General picture
(...) I will use your recommendations to improve and review the management and day-to-day implementation of the cloud policy and implementation framework. I will centralise the activities to be taken for this process. All ministries and their units, however, must carry out the activities under the direction of their own ministers and senior civil servants.

All ministries and their units: Improvement operation: more insight and better risk control
You observe that insight into cloud use and risk control are still inadequate. The summaries drawn up by the ministries and their units are not yet complete and important insights are consequently lacking. Furthermore, not all units share their summaries with their ministry and do not share summaries of material cloud use with CIO-Rijk. In many cases, risk analyses have not been made. Partly for this reason, the measures taken have fallen short of expectations.

Operational control is a responsibility of the ministries concerned. You note that improvements were made between the two measurement moments. I will take action with my colleagues to accelerate the improvements already being made and so improve ministerial insight into cloud use and strengthen risk control. I will provide support from the centre. Better insight into individual risks will provide an opportunity to control interministerial risks and take account of them in the study on digital autonomy.

Preparations for future cloud use will also take account of your findings and recommendations. For instance, SSC-ICT is updating the workplace services you audited. In keeping with the agreements made with the House, no irreversible steps will be taken in this process. The risks of all planned cloud use will be mitigated in advance.

Introduction of the General Security Requirements for Central Government Contracts (ABRO) will also improve the mitigation of cloud risks. By default, service delivery and the service provider will be subject to more requirements. The service delivery and provider's fulfilment of the requirements will also have to be verified.

Min BZK and the ministries: Improve management and supervision
In view of the weak operational control, you recommend that management and supervision should not be discretionary.

I agree that operational improvement requires better management and supervision. To manage the progress of operational improvement, I have taken measures to have CIO-Rijk periodically inform me of ongoing developments. Where necessary, I will make adjustments together with my colleagues. Where a national interest or national security is concerned, I will seek to strengthen the relationship between central government entities. CIO-Rijk will coordinate the process and facilitate oversight of improvement measures by the CIOs in central government.

Min BZK: Improve policy and extend scope
Although many of the above findings will be resolved by the full implementation of the cloud policy and implementation framework, you believe policy can be improved by making it more uniform and specific. This can be achieved chiefly by reducing the differences in ministerial cloud documents, by extending the scope to all of government, including local authorities and ZBOs, and by excluding certain public services from the cloud.

I support the idea of a unified central government and want the review of cloud policy to consider local authorities and ZBOs, and to arrive at a single cloud policy for all of government. This idea will also be included in the Netherlands Digitalisation Strategy (NDS), which is currently being worked out.

In principle, I am in favour or making policy more specific and uniform. It agrees with my own evaluation. I will include these points in the forthcoming review of central government's public cloud policy. Reducing the differences between ministerial policy documents and excluding specific services are worthwhile recommendations. Much more uniformity is possible at strategic policy level. At the same time, the undeniable operational differences between central government organisations lead to different functional demands on cloud use. Furthermore, there is more than one way to perform operationally sound risk control. These opportunities must be retained. A one-size-fits-all approach may be appropriate at strategic level but not always at operational level. It is important to strike the right balance.

Min BZK and ministries: Improve cooperation in procurement and contract management

You observe that strategic vendor management (SLM) is insufficiently consulted and contractual agreements are complex. You recommend making more use of joint procurement, with SLM playing a key role, and seeking cooperation at EU level.

I agree with the importance of greater cooperation in procurement and strengthening the role and position of SLM, for example by means of a shared expertise centre and a specialised external or internal service. This would result in a set of formal agreements, a logical structure and hierarchy, fewer contracts and hence less complexity. A balanced and comprehensive set of measures (technical, internal procedures, agreements with vendors, etc.) would better safeguard autonomy, continuity and data protection. Cooperation would increase effectiveness in this area.

The EU has been contacted with regard to cooperation and we will remain in contact. We are working together in various areas, including the cloud and studies of EU cloud initiatives.

I gladly invite you to discuss the approach and follow-up to your findings with me.'

7.2 Afterword

We appreciate the state secretary's response that he shares our main conclusions that central government cloud use is worrying and improvement is needed. He acknowledges that more management and supervision is required from him. We will gladly accept the state secretary's invitation to remain in discussion at technical and political level. He can make improvements more specifically and with greater urgency in several areas.

The House of Representatives is understandably concerned about digital sovereignty. Exclusion of certain services from the public cloud would therefore be appropriate. In accordance with central government cloud policy, classified information is already excluded. Base registries are subject to the 'no by default' principle. The individual ministries could exclude services, such as vital physical infrastructure. The *Organisation, Operational Management and Information Systems Coordination Decree* and the *CIO-Rijk System Decree* allow the state secretary to decide which services should be excluded. This would not limit the line ministries' ministerial responsibilities. In the longer term, a sovereign cloud could offer a partial solution to this, with the assistance of European cloud providers or otherwise. The state secretary could also issue a binding definition of material public cloud use and take the lead in joint procurement of the cloud.

In this light, our second and final point relates to the state secretary's fulfilment of his own role. It is positive that he wishes to address his colleagues but before doing so he should officially make other ministries aware of their responsibilities under central government's mandatory cloud frameworks. Risk assessments of cloud use, for instance, are already compulsory and must still be performed within a given, short, period of time. If they do not lead to improvements, the aforementioned Coordination Decree could be escalated to the Cabinet. Too little use is made of the Minister of BZK's mandate. Transparency regarding the situation at each ministry would also lead to improvement. After all, it is unacceptable to place sensitive information in the cloud without a risk assessment. Misuse of the information by malicious or state actors must be prevented at all times. Citizens and businesses have a right to expect central government to treat their data with care.

Appendices

Appendix 1 Methodology

What dit we audit?

We carried this audit out in order to answer 2 key questions. The first relates to the measures taken across central government to implement central government cloud policy and the implementation framework.

Key question 1: To what extent do CIO-Rijk and the ministries' CIOs comply with certain aspects of central government cloud policy and the implementation framework?

The 'certain aspects' are listed below. To ensure the audit remained feasible, we selected those aspects of central government cloud policy and the implementation framework that in our opinion should at least be satisfied. We investigated the extent to which the ministries had:

- formalised a cloud policy: CIO-Rijk's cloud policy requires every ministry to have its own cloud policy;
- an insight into their cloud use: a ministry must have an insight into the cloud services it uses and/or have made contractual agreements on its cloud services;
- assessed the advantages and disadvantages (including costs) of public cloud contracts: a ministry must make a risk assessment and prepare a business case for cloud contracts wherever possible.

We then investigated whether the ministries satisfied those aspects of central government cloud policy and the implementation framework that we audited.
We investigated measures taken by:

- the Minister of BZK regarding CIO-Rijk's responsibilities;
- the Minister of BZK and the other ministers regarding the measures taken by the ministries' CIOs.

The audit framework in appendix 2 explains how these aspects relate to central government cloud policy, the implementation framework and associated responsibilities.

We requested information on all forms of the cloud, not only the material public cloud, which is subject to central government cloud policy. We also investigated the situation at the Ministry of Defence, which is not formally subject to the policy.

The second key question relates to central government's safeguarding of the 3 principles.

Key question 2: To what extent do the 3 selected public cloud contracts safeguard digital sovereignty, business continuity and data protection?

To answer this question, we selected 3 cloud contracts[33] from among those named in answer to key question 1, most of which were for public clouds, and that had the most relevance to the delivery of public services to citizens and businesses.
Our intention was to carry out a representative audit within a realistic timeframe.
The ministries had to satisfy us that they had acted appropriately to safeguard the 3 principles of digital sovereignty, business continuity and data protection. We did not use the findings to make generalising statements on all central government cloud contracts. However, our audit did provide a reliable indication of how safeguards can be used to sharpen up cloud policy and the implementation framework.

The criteria we applied were consistent in so far as possible with central government cloud policy and the implementation framework. We also applied supplementary criteria based on relevant laws and regulations. In addition, we organised a workshop with experts to refine the audit framework.

We examined the service delivery agreements laid down in the 3 public cloud contracts or in user agreements, service conditions and other documents. More particularly:

- to audit the SSC-ICT’s contract, we investigated the contract and service agreements with Microsoft;
- to audit CIBG’s contract: we analysed CIBG’s contractual agreement with its main cloud contractor. The underlying documents, such as the Service Level Agreement and the Agreement and Procedures File, include agreements on the services a subcontractor will perform for KLOPT. The subcontractor also approves the Agreement and Procedures File. References in this report to this contract are to the contractual agreements between VWS/CIBG and the main contractor and subcontractor;
- to audit KNMI’s contract, we looked primarily at the contract between KNMI and SURF because KNMI had made contractual arrangements with SURF in a framework agreement. SURF is the contractor in the chain of service providers and has been designated by KNMI as the reseller. In accordance with its contractual agreements with KNMI, SURF has concluded contracts with other organisations for KNMI to use the AWS cloud services.

Context / opportunities and risks

To gain a proper, balanced picture of the opportunities and risks of the cloud, we held interviews with the Cyber Security Council, cloud service providers, the Dutch Personal Data Authority, policy-makers at the European Commission and other stakeholders.

Audit fieldwork

- The audit was carried out between May 2023 and the end of August 2024.
- The audit was launched with presentations to central government bodies: the CISO Council, the CTO Council and the CIO Committee. We then undertook the following actions:
- We drew up a cloud overview template (included in appendix 2) to take stock of the cloud services in use at all 11 ministries.
- We requested and analysed ministerial policy and assessment frameworks, overviews of cloud use and risk assessments of public cloud contracts from all 11 ministries.
- We held introductory talks and interviews with relevant officials at all ministries to clarify the information they had provided in their cloud overviews.
- We prepared a framework to audit the 3 contracts based on input and analyses of the criteria and relevant developments.
- On 28 September 2023, we organised a workshop on the control framework

applied to audit the 3 contracts. Together with the participants, we identified the criteria we would use. The workshop had 31 participants from most of the ministries and also auditors from the Central Government Audit Service and advisers from the SLM and the NCSC. The framework was then refined based on the workshop and further investigation.

- We requested and analysed contract documents and the audit framework prepared for the 3 selected public cloud contracts.
- We held introductory talks and interviews with relevant officials from the ministries to clarify the information they had provided for the audits of the 3 contracts.
- During the audit period and before and after the various talks and interviews, we requested and analysed documentation from the auditees.
- Expert interviews: in the second half of 2023 and the first half of 2024, we interviewed several central government and non-governmental cloud technology experts. Talks were held with officials from the NCSC, the European Union Agency for Cybersecurity (ENISA), SSOs and EY. A full list of interviewees is given in appendix 3.
- Cloud seminar: to audit policy, oversight and assessment, we prepared 2 memoranda for each ministry: 1 regarding the situation at the end of 2023 and 1 regarding the situation in mid-2024. On 8 February 2024 we organised a seminar to discuss the findings on the situation at the end of 2023, so that ministries could make improvements in the months that followed.
- For this audit we prepared 26 reports of findings on the various audit subjects and ministries. Those reports informed this report.

Appendix 2 Audit frameworks

Audit framework for key question 1

The audit framework we used to answer key question 1 is presented below. The Criteria column lists the criteria we checked in order to answer the key question. The Risk column identifies the risk and the measures necessary to meet the agreed criteria. The Sources column is a non-exhaustive list of sources of measures to meet the criteria. The Reference column show the criteria's source and the **Audit procedures** column describes the actual check.

Key question 1: *To what extent do CIO-Rijk and the ministries' CIOs comply with certain aspects of central government cloud policy and the implementation framework?*

Criteria 1	Risk	Sources	Reference	Audit procedures
CIO-Rijk monitors the implementation of central government cloud policy and reports to the House of Representatives	Risk that organisations do not correctly implement or are not aware of central government cloud policy. The organisation then runs digital sovereignty, business continuity and data protection risks.	• Interviews with CIO-Rijk. • Communication of central government cloud policy. • Monitoring checks.	Central government cloud policy 2022, condition 1: *'CIO-Rijk monitors implementation in accordance with the CIO System Decree*'. Implementation framework Article 14: '*In the annual CIO interview cycle, CIO-Rijk uses the reports, DPIAs and risk analyses it receives in accordance with the cloud policy and the CIO system, as part of its monitoring and advisory function.* *Based on the reports it receives, CIO-Rijk keeps a comprehensive overview of material public cloud use. In accordance with the cloud policy, CIO-Rijk informs the House of Representatives of the progress made implementing cloud policy.'*	We checked whether CIO-Rijk: • monitored implementation of cloud policy; • held interviews to discuss the cloud; • analysed and responded to monitoring information; • kept a comprehensive overview of material public cloud use; • informed the House of Representatives of the progress made implementing cloud policy.

Key question 1a: ministerial cloud policy

Criteria 2	Risk	Sources	Reference	Audit procedures
All government ministries formulate their own cloud policy and strategy subject to central government cloud policy and the implementation framework.	Risk that cloud policy and strategy are not implemented or are not consistent with central government cloud policy with regard to digital sovereignty, business continuity and data protection.	• Ministerial cloud policy and strategy. • Other ministerial frameworks on cloud use. • Interviews at each ministry (interview minutes).	Cloud implementation framework: Art 1.b	We checked whether ministerial cloud policies and strategies: • were present, • had been formalised, • incorporated central government cloud policy. We did not check whether ministerial policies and strategies were fully consistent with central government cloud policy and the implementation framework.

Key question 1b: a cloud overview

Criteria 3	Risk	Sources	Reference	Audit procedures
For their material public cloud use, the ministries keep a record of at least: a. the organisational unit, b. the business process, c. insight into risks, d. the public cloud service provider and the cloud services concerned.	Without such a record, the organisation cannot comply with laws and regulations, including risk management and disclosure notifications.	• Cloud overviews received from the ministries in accordance with the template. • Other documentation relating to a, b, c and/or d. • Interviews at each ministry (interview minutes).	Cloud implementation framework: Art 13.1	We checked whether the ministries kept a record of their cloud use, in any event including material public cloud services and the relevant organisational unit or business process, stating whether a risk assessment had been made and who the cloud provider was. We checked material public cloud use (the standard). At least an overview of material public cloud use had to be present.

Key question 1c: a formalised assessment of advantages and disadvantages (including costs)

Criteria 4	Risk	Sources	Reference	Audit procedures
The ministries and their units have formalised a risk management method in accordance with the BIO. A risk assessment is made in accordance with the method before a public cloud is used. In accordance with the cloud policy, SLM is consulted regarding the re-use of previous analyses and a joint approach is taken where possible. The decision to formalise a cloud policy also assessed costs and benefits.	If a decision is not well-considered, there is a risk that data will not be protected, and business continuity and the organisation's independence cannot be guaranteed. If the costs are not known and a master agreement is not used, the services may be more expensive and may be inconsistent with central government agreements.	• Documentation on assessments, risk management and/or financial aspects. • Interviews at each ministry (interview minutes).	Cloud implementation framework: Art. 4.1 and 2 Additional by Court of Audit	We checked for the following elements: • for 'risk management method' 1. was a method present? a. was a strategic assessment made of cloud use? b. did the method relate specifically to the cloud? 2. had the method been formalised? • for risk assessments of material public cloud services: 1. had risk assessments been made? a. in accordance with the method, or b. otherwise? (A risk assessment can be made as part of a risk analysis). 2. was SLM consulted? 3. were financial aspects (costs/ benefits) included in the assessment?

Audit framework for key question 2

The audit framework applied to answer key question 2 is presented below. The **No.** column refers to a criteria's unique number, as used in chapters 4, 5 and 6 and to the 3 principles of sovereignty (Sn), continuity (Cn) and data protection (Dn). The 3 principles and associated risks are defined at the end of this appendix. The **Control domain** column states the criteria's domain. The **Source + Control ID** column names the source of the criteria, which could be a central government framework or cloud-related good practices. The subjects are summarised at the end of this appendix. The **Criteria** column lists the controls we audited. The **Audit procedures** column shows our fieldwork regarding the design and implementation of controls.

Key question 2: *To what extent are digital sovereignty, business continuity and data protection safeguarded in the 3 selected public cloud contracts?*

No.	Control domain	Source + Control ID	Criteria	Audit procedures
S1	Contract closure	Ministry of the Interior and Kingdom Relations – Cloud Implementation Framework	Conclusion of the contract was preceded by a risk assessment. The contract states who is responsible at the CSC and the CSP for contract management.	**Design** 1. Establish that the CSC has prepared a risk assessment for the cloud service to be purchased. 2. Establish that the CSC has insight into the chain of parties involved for service delivery up to and including the CSP. 3. Establish that the contractual arrangements include the roles and responsibilities of the CSC, CSP and other chain parties on the management of the contract. **Implementation** 1. Establish that the CSC has determined that measures are included in the contract for key risks. 2. Establish that any changes to the contract have taken place in accordance with agreed roles and responsibilities.

No.	Control domain	Source + Control ID	Criteria	Audit procedures
S2	Interoperability & Portability	CCM IPY-01	Interoperability and portability are included in the cloud service agreement, with agreements established for: a. roles and responsibilities of the CSP and the CSC on interoperability and portability; b. interoperability of data exchange and processing; c. portability of cloud systems.	**Design** 1. Establish that the contract contains arrangements on the roles and responsibilities of the CSP and CSC regarding interoperability and portability. 2. Establish in the contract how interoperability of data exchange and processing will be ensured. 3. Establish that the contract specifies how the portability of cloud systems will be ensured. **Implementation** 1. Establish that the CSP periodically reports to the CSC on status and changes on interoperability and portability. 2. Establish that the CSC periodically tests interoperability of data exchange and processing. 3. Establish that the CSC periodically tests the portability of cloud systems..

S3	Interoperability & Portability	CCM IPY-04;
		SWIPO CCCDPCSS 4.4;
		SWIPO CCCDPCSS 5.7;
		SWIPO CCCDPCSS 5.16
			CSCs' access to data upon contract termination are included in the cloud service agreement and include:
			a. data format in accordance with Open Standards;
			b. time period during which data will be stored;
			c. scope of data stored and made available to CSCs;
			d. data deletion policy;
			e. encryption of the export file.
				Design
				1. Establish that the contract contains agreements on CSC's access to data upon termination of the contract, with at least agreements on the five aspects from the standard.
				Implementation
				1. Establish that the CSP periodically demonstrates compliance with the agreements to the CSC..

S4	Interoperability & Portability	EDPS	The CSP must ensure and demonstrate that the CSC's data from its systems and each sub-processing system is transferable to other CSPs within the time and format agreed upon in the cloud service agreement, at the CSC's option.	**Design** 1. Establish that the contract includes agreements, regarding time and format, for transferring data from the CSC to other CSPs. **Implementation** 1. Establish that the CSC determines that the CSP periodically demonstrates that time and format agreements have been met. 2. Establish that the CSC determines that the data is transferable to another CSP.

No.	Control domain	Source + Control ID	Criteria	Audit procedures
S5	Disclosure notification	CCM DSP-18	The procedure for managing and responding to requests for disclosure of personal data by law enforcement authorities in accordance with applicable laws and regulations has been established by the CSP and communicated to the CSC. In doing so, the CSP highlights the notification procedure to interested CSCs unless otherwise prohibited, such as a prohibition under criminal law to maintain the confidentiality of a law enforcement investigation.	**Design** 1. Establish that the roles and responsibilities of the CSP and the CSC on requests for disclosure of persona) data by law enforcement authorities are specified in the contract. 2. Establish that notification procedures regarding disclosure of personal data are specified in the contract. **Implementation** 1. Establish that in the case of disclosure of personal data by law enforcement authorities, notification procedures have been followed.
S6	Data Location and Data Flow	CCF 79; CCM DSP-19; CCF 114; CCM DSP-05	- The CSC identifies geographic areas of regulatory risk, such as embargoed countries. - The CSP has defined procedures and measures to specify and document the physical locations of data, including locations where data is processed or backed up. - The CSP transfers data from the CSC to a country outside the European Economic Area (EEA) only if agreed as part of the Cloud Service Agreement. - Documentation on data flows are in place to determine what data are processed, stored or transmitted where.	**Design** 1. Establish that the CSC has identified geographic risk areas for data processing and storage. 2. Establish that the contract documents the physical locations of data processing, storage and backups. 3. Establish that the contract includes arrangements for the transfer of data from the CSC to countries outside the EEA. 4. Establish that the CSC has documented data flows (transmission, processing and storage). **Implementation** 1. Establish that the CSC determines that data processing, storage and backups occur only at the documented physical locations.
S7	Right to audit	CCF 3; DEDPS	Procedures related to audits requested by the CSC are defined, documented and transparently communicated to the CSC and, if applicable, the mandated auditor.	**Design** 1. Establish that the right to audit with the CSP and potential sub-processors and the terms under which cost and time limit are included in the contract. **Implementation** 1. Establish that the right to audit can be applied in practice.

No.	Control domain	Source + Control ID	Criteria	Audit procedures
C1	Business Continuity Management and Operational Resilience and Multi-Location Strategy	CCM BCR-01 CCM BCR-02 CCM BCR-03 CCM BCR-04 CCM BCR-06 CCM BCR-09 CCM BCR-10 CCF 19	The CSC and CSP have defined procedures and measures for business continuity management and include: - a risk analysis underlying the procedure; - a business continuity plan; - business continuity testing; - disaster recovery plan; - disaster recovery testing. The cloud service agreement includes arrangements for a multi-location or region strategy for production environments to resume operations at other CSP facilities if a facility fails.	**Design** 1. Establish that the roles and responsibilities of the CSC and the CSP on BCM are defined in the contract. 2. Establish that the contract defines the procedures and measures about BCM, including: risk analysis, business continuity plan and testing, disaster recovery plan and testing and multi-location or region strategy are a part of BCM. **Implementation** 1. Establish that the CSC has prepared a risk analysis for BCM. 2. Confirm that the BCP has been established, communicated and is periodically reviewed and updated. 3. Establish that business continuity testing has taken place over the past year. During testing, locations from the multi-location strategy were included. 4. Confirm that the disaster recovery plan has been established, communicated and is periodically evaluated and updated. 5. Establish that disaster recovery testing has taken place within the past year. 6. Establish that the multi-location or region strategy is periodically tested during BCM testing, disaster recovery testing and backup testing.

No.	Control domain	Source + Control ID	Criteria	Audit procedures
C2	Backup and data replication	CCM BCR-08 and CCF 23	The cloud service agreement includes arrangements on responsibilities regarding regular backups of data stored in the cloud. The cloud service agreement includes arrangements on replication to a secondary database or data centre	**Design** 1. Establish that the cloud service agreement defines the roles and responsibilities for regular data backup. 2. Establish that the cloud service agreement defines the manner in which periodic testing of data recovery from backup is performed. 3. Establish that the cloud service agreement defines the manner in which data replication to a secondary database or data centre occurs. **Implementation** 1. Establish that the CSC determines that backup by the CSP has been made in accordance with the agreements. 2. Establish that the CSC periodically tests the recovery of data via backup. 3. Establish that the CSC establishes that data replication has occurred to a secondary database or data centre.
C3	Change management	CCM CCC-01 BIO 12.1.2	The cloud service agreement includes arrangements on applying changes to company assets, including applications, systems, infrastructure, configuration, etc. In doing so, responsibilities are made explicit.	**Design** 1. Establish that the roles and responsibilities of the CSP and the CSC regarding change management are defined in the contract. 2. Confirm that the contract describes the change management process. **Implementation** 1. For a number of changes, establish that these changes have taken place in accordance with roles, responsibilities and process.

No.	Control domain	Source + Control ID	Criteria	Audit procedures
C4	Security Incident Management, E-Discovery, & Cloud Forensics	CCM SEF-03	The CSC and CSP have defined procedures and measures for security incident response and include: - affected parties; - relevant business-critical relationships (such as supply chain) that may be affected.	**Design** 1. Establish that the roles and responsibilities of the CSP and the CSC regarding security incident and event management are defined in the contract. 2. Confirm that the contract describes the security incident and event management process. **Implementation** 1. For a number of incidents, establish that these incidents occurred in accordance with roles, responsibilities and process.
G1	Governance Management	CCF 115 CCM STA-01	The cloud service agreement includes arrangements on the roles and responsibilities of CSP and the CSC. The agreement includes definitions, including but not limited to: - responsibilities for granting access and approval; - use by (sub)suppliers.	**Design** 1. Establish that the roles and responsibilities of the CSP and the CSC regarding data protection are defined in the contract, regarding responsibilities for granting access and approval and use by (sub) suppliers. **Implementation** 1. Establish that access is granted for data in accordance with agreed roles and responsibilities.
G2	Cryptography, Encryption & Key Management - encryption algorithm	CCM CEK-03; CCM CEK-04 CCF 89	The cloud service agreement includes arrangements on encryption algorithms and key management suitable for data protection, taking into account the classification of data. The cloud service agreement includes agreements on cryptographic protection for 'data at rest' , 'data in motion' and 'data in use', using cryptographic libraries certified to approved standards.	**Design** 1. Establish that the contract specifies data classification. 2. Establish that the contract specifies the encryption algorithms, encryption standards and key management in accordance with the classification of the data. Confirm that this is laid down for 'data at rest', 'data in motion' and 'data in use'. **Implementation** 1. Establish that CSC has determined that an encryption algorithm/ encryption technology is being used, in accordance with the contract. 2. Establish that CSC has determined that key management is performed in accordance with the arrangements in the contract.

No.	Control domain	Source + Control ID	Criteria	Audit procedures
G3	Identity & Access Management	CCM IAM-01 CCM IAM-02 CCM IAM-08 CCF 164 BIO 9.2.2 BIO 9.2.3 BIO 9.4.3	The cloud service agreement includes arrangements on tasks, roles, authority and responsibilities regarding access management at the CSC and CSP. The cloud service agreement and also includes agreements on: - identification and authentication; - password policy; - "least privilege" and segregation of duties; - special access rights, including highly privileged accounts; - access and use of vendor accounts only for the period required and monitoring during use.	**Design** 1. Establish that the contract specifies agreements on duties, roles, authority and responsibilities regarding access management at the CSC and the CSP. 2. Establish that the contract includes agreements on at least: - identification and authentication; - password policy; - "least privilege" and segregation of duties; - special access rights, including highly privileged accounts; - access and use of vendor accounts only for the period required and monitoring during use. **Implementation** 1. Determine that access management has been performed by the CSC and CSP in accordance with the agreements on duties, roles, authority and responsibilities established in the contract. 2. Establish that the CSC determines that contract requirements are met in practice, including identification and authentication, password policies, least privilege and job segregation, special access rights with highly privileged accounts, and access and use of vendor accounts only for the period of time required and monitoring during use.

No.	Control domain	Source + Control ID	Criteria	Audit procedures
G4	Supply Chain Management, Transparency, and Accountability	CCM STA-08	The cloud contract includes arrangements on periodic assessment of risk factors related to the organizations within the supply chain.	**Design** 1. Establish that the contract specifies how and by whom a periodic assessment of risk factors related to the organizations within the supply chain will take place. This shall take place at least every three years or when there are substantial changes in cloud service provision or risk factors. **Implementation** 1. Establish that the CSC has conducted a periodic assessment of risk factors related to the organizations within the supply chain. 2. Establish that the periodic assessment has taken place within three years or upon material changes in cloud service delivery or risk factors.
G5	Threat & Vulnerability Management	CCM TVM-01	The cloud contract includes arrangements on vulnerability management: - detect vulnerability; - assess the risk; - prioritize remediation; - confirm remediation.	**Design** 1. Establish that the cloud contract defines duties, roles, authority and responsibilities regarding vulnerability management. **Implementation** 1. Establish that the CSC determines that vulnerabilities of the cloud environment are periodically monitored and that identified vulnerabilities and remedial actions are adequately followed up.

No.	Control domain	Source + Control ID	Criteria	Audit procedures
G6	Infrastructure & Virtualization Security	CCM IVS-06	The cloud contract includes agreements on the arrangement of applications and infrastructure, whereby different customers' access to services and resources within a cloud environment are - are appropriately segmented and separated; - is monitored; - is not accessible to other customers.	**Design** 1. Establish that the cloud contract specifies arrangements for the design of applications and infrastructure whereby access by different customers to services and resources within a cloud environment:: - are appropriately segmented and separated; - is monitored; - is not accessible to other customers. **Implementation** 1. Establish that the CSC determines that the cloud environment is segmented and segregated for different customers. 2. Establish that it has been monitored that customers have only been granted access to services and resources in the cloud environment designated for them. 3. Establish that other customers did not access services and resources not intended for them (= break segmentation).3. Check that other consumers do not have access to services and resources not intended for them (= breach of segmentation).

Legend: Source + Control ID

This framework draws on a variety of sources and makes specific reference to the control ID:

- CCM: Cloud Control Matrix (CCM, version 4.0.7). Source: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.
- CCF: Cisco Cloud Controls Framework (CCF, Public Release V2.0). Source: https://www.cisco.com/c/en/us/about/trust-center/compliance/ccf.html
- SWIPO: Converged Code of Conduct for Data Portability and Cloud Service Switching (version 2023 - v.1) SWIPO, Switching Cloud Providers and Porting Data is a multi-stakeholder group facilitated by the European Commission, in order to develop voluntary Codes. Source: https://swipo.eu/wp-content/uploads/2023/06/SWIPO_AISBL_ConvergedCode-v1._29.03.2023_For-publication_Final.pdf
- BIO: Central government Information Security Baseline (BIO version 1.04);
- BZK Cloud Implementation Framework 2022;
- European Data Protection Supervisor - Guidelines on the use of cloud computing services.

Abbreviations in the audit framework

- CSC: Cloud service consumer. The cloud service provider's consumer, in this case the ministry concerned.
- CSP: Cloud service provider. In this case the provider of the underlying cloud service, the hyperscalers.
- Chain: The CSC, CSP and any intermediaries and resellers (which can also be considered partial CSPs).

Appendix 3 Organisations interviewed

Besides interviewing staff at all the ministries and some executive organisations, we held talks with experts in the cloud at the following organisations. For privacy reasons, only 2 of the experts are named.

In alphabetical order:

1. Bert Hubert (entrepreneur & software developer, see https://berthub.eu/)
2. Cyber Security Council (CSR)
3. Dictu (ICT Services)
4. Dutch Personal Data Authority
5. European Commission, Directorate-General Communications Networks, Content and Technology (DG CNET)
6. European Data Protection Board (EDPB)
7. European Union Agency for Cybersecurity (ENISA)
8. EY
9. National Cyber Security Centre (NCSC)
10. Netherlands National Communications Security Agency (NBV)
11. Netherlands Standardisation Forum
12. ODC-North
13. SSC-ICT (Share Service Centre-ICT)
14. Thales

Appendix 4 Definitions and abbreviations

The terms and abbreviations used in this report are explained and defined in the table below. The source on which the description is based is also given.

AWS – Amazon Web Services (AWS) is a web services and cloud computing subsidiary of the American company Amazon.com. Source: Wikipedia

Azure – Microsoft Azure Platform is a cloud computing platform of the American company Microsoft that offers a number of services over the internet or within an organisation's environment. Source: Wikipedia

Business continuity management – Business continuity management (BCM) is the process of identifying potential threats and calculating their impact on an organisation's operations should the threat materialise. BCM provides a framework to withstand the threats, in part through effective response. Source: Wikipedia

Change management – The procedure (submission, analysis and decision-making) that describes the response to change proposals. The change can relate to an application, platform or infrastructure. Source: Internet

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

Cloud service consumer (CSC) – The consumer of a cloud service, in this audit a ministry. Source: Netherlands Court of Audit

Cloud service models – The 3 most important service models for the cloud are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Each service model meets the needs of its target users and organisations and offers different levels of control, security and scalability. See also the definitions of the individual service models, Community cloud and Hybrid cloud. Source: Internet

Cloud service provider (CSP) – De organisation that provides the underlying cloud services, in this case the hyperscalers. 2 well-known hyperscalers are AWS and Azure. See also: AWS, Azure and hyperscaler. Source: Netherlands Court of Audit

Community cloud – Cloud infrastructure provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises. See also: Cloud service models and Hybrid cloud. Source: NIST

Business continuity – The delivery of public services is not jeopardised. Key aspects are:

- *Interoperability*. This is the ability of IT systems to work with other IT systems so that data can be shared and further processed, facilitated by the use of open standards and open source.
- *Prevention of vendor lock-in*: over-reliance on 1 vendor. Portability is an important aspect: data can be transferred to another vendor and a realistic exit strategy is in place.

Source: Netherlands Court of Audit

Cryptography – Cryptography is used to transfer data that may not be read by other parties. Only the recipient, and possibly the transmitter, has the key to decrypt the data and restore them to their original form. Source: Wikipedia

Service provider – Organisation that provides a cloud application. Source: NCA

Disclosure notification – Notification of public disclosure by a cloud service provider. Notification procedures are relevant when:

- law enforcement authorities request access to personal data stored in the cloud;
- legal procedures or official investigations require the disclosure of client data;
- summonses or court orders require the cloud service provider to disclose information to authorised parties.

Source: Internet

Europese Economic Area (EEA) – The European Economic Area (EEA) comprises all EU member states plus Lichtenstein, Norway and Iceland. Source: Internet

Data protection – Adequate protection of data. In a public cloud, ownership of software and hardware and sometimes the data usually does not lie with a central government organisation itself. Availability, confidentiality and integrity of the data are then important. Source: Netherlands Court of Audit

Hybrid cloud – The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique units but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). See also: Cloud service models and Community cloud. Source: NIST

Hyperscaler – An organisation that provides hyperscale computing. Hyperscale computing is necessary to build a robust scalable cloud, big data, map reduce or distributed storage system and is often associated with the infrastructure required to run large distributed sites such as Google, Facebook, Twitter, Amazon, Microsoft, IBM Cloud or Oracle. Seer also: Cloud service provider (CSP).

Identity and access management – Identity and Access Management (IAM) is required to ensure the right identities (chiefly persons or computers) have access to the right facilities for the right reasons at the right time. Source: NORA

Infrastructure as a Service (IaaS) – Type of cloud service model. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). See also: Cloud service models. Source: NIST

Cloud service provider chain – A cloud service provider chain is the chain of services, equipment and information provided by vendors via an organisation to its clients. The organisations in the chain turn a resource into a product and/or service. Links in the cloud service provider chain include the cloud service consumer (CSC), cloud service provider (CSP) and any intermediaries and resellers (who are also considered to be partial CSPs). Source: Internet / Netherlands Court of Audit

Materiel public cloud use – Material public cloud use is the use of public cloud services to perform an organisation's primary task. The cloud service is of critical importance to the organisation. It support business processes as far as they enable the primary task. Source: BZK

Subcontractor – A subcontractor is a person or organisation that commits to perform part or all of another party's contract obligations. A subcontracting contract assigns part of an existing contract to a subcontractor. Source: Wikipedia

On-premise – On-premise software is installed and run on an organisation's own hardware infrastructure and is hosted locally. Cloud software, by contrast, is stored and managed on the provider's servers and is accessible by means of a web browser or other interface. Source: Internet

Pentest – A penetration test or pentest is a test of one or more computer systems for vulnerabilities that are then used to hack the systems.
One characteristic of a pentest is that it is performed occasionally on request. A pentest is a combination of automated and annual tests. See also: Vulnerability management. Source: Wikipedia and Netherlands Court of Audit

Platform as a Service (PaaS) – Type of cloud service model. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. See also: Cloud service models. Source: NIST

Private cloud – The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. Source: NIST

Public cloud – The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or central government organization, or some combination of them. It exists on the premises of the cloud provider. Source: NIST

Reseller – A reseller is an organisation authorised by a cloud service provider to resell licences. A reseller can be engage by a cloud service consumer to hep procure and/or implement the cloud service. Source: Netherlands Court of Audit

Right to audit – A provision in a contract that gives a party the right to audit another contract party. The audit is usually performed by an independent third party. Source: Internet

Risk assessment – A risk assessment is a method to quantify the strategic risk of cloud use by calculating the probability of a threat occurring and the consequences: Risk = Probability x Impact. A risk assessment has to be made before an organisation decides to use a cloud service. Source: Netherlands Court of Audit

Risk analysis – A risk analysis is a method to quantify the operational risk of cloud use by calculating the probability of a threat occurring and the consequences: Risk = Probability x Impact. A risk analysis has to be made before an organisation decides on its cloud use.Source: Netherlands Court of Audit

Security incident – An information security incident is one or more undesirable or unexpected events with a high risk of forming a threat to a business process and/or to the availability, integrity and/or confidentiality of data. Source: Internet

SLM – A strategic vendor management organisation is the initiator of central government contracts and procurement conditions for software and cloud services. The agreements are laid down in master agreements with IT vendors. SLM is fragmented. The Ministry of J&V, for example is responsible for the Microsoft, Google Cloud and Amazon Web Services. The Ministry of EZ (DICTU) is responsible for Oracle and the ministry of Finance (Tax and Customs Administration) for IBM. Source: SLM

Digitial sovereignty – The capacity to take autonomous decisions and actions concerning essential digital aspects of the economy, society and democracy, i.e. the use and design of digital systems and the data they generate and store and related business processes. Source: Netherlands Court of Audit

Software as a Service (SaaS) – Type of cloud service model. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a

program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. See also: Cloud service models.
Source: NIST

State actors – State actors are countries that use digital espionage to attack targets in public and private sectors at home and abroad. Activities include attacks on digital parts of the vendor chain. Unlike cybercriminals, state actors have unlimited time and money to exploit vulnerabilities. Source: Internet

Tenant – A cloud tenant is an individual or organisation that subscribes to and uses services provided over a cloud computing platform. The services include virtual machines, storage and software. Tenants share the same infrastructure in a safe and isolated manner. Source: Internet

Virtuele machine – Virtual machineA virtual machine is a computer program that emulates a computer and on which other programs can be executed. Source: Wikipedia

Vulnerability management – Vulnerability management is the process of identifying, evaluating, responding to and reporting on security weaknesses in systems and in the software that runs on them.
Vulnerability scans are usually automated and performed very regularly. This is in contrast to pentests, which are also performed manually and more occasionally. See also: pentest. Source: Internet and Netherlands Court of Audit.

Appendix 5 References

Dutch Personal Data Authority (2022). *Inzet van Cloud Service Providers [Use of Cloud Service Providers*]. Reference z2022-00846. The Hague: self-published

Dutch Personal Data Authority (2023). *Beleidsreactie Advies Autoriteit Persoonsgegevens inzake het Rijksbreed Cloudbeleid 2022* [Policy response to Personal Data Authority advisory report on central government cloud policy 2022]. Reference 2023-0000028460 The Hague: self-published

Central Government Audit Service (2024). *Onderzoeksrapport Evaluatie public cloudbeleid Rijksoverheid* [Audit report, Evaluation of central government public cloud policy]. The Hague: self-published

Netherlands Court of Audit (2020). *Factsheets: Grip op digitalisering: rode draden uit tien jaar Rekenkameronderzoek* [Factsheets: Control of digitalisation: common threads of ten years of Court of Audit audits]. The Hague: self-published

Netherlands Court of Audit (2024). *Focus op AI in the Dutch central central government.* The Hague: self-published

BZK (2021). *I-strategie Rijk 2021-2025* [Central government i-strategy 2021-2025]. The Hague: self-published

BZK (2022). *Rijksbreed cloudbeleid 2022* [Central government cloud policy 2022]. House of Representatives 2021-2022 26 643 no. 904

BZK (2023a). *Beantwoording Schriftelijk overleg over het Rijksbreed cloudbeleid 2022* [Answer to written consultation on central government cloud policy 2022]. House of Representatives 2022-2023 26 643 no. 963

BZK (2023b). *Implementatiekader risicoafweging cloudgebruik* [Cloud use risk assessment implementation framework]. House of Representatives 2022-2023 26 643 no. 964

BZK (2023c). *Beleidsreactie op een brief van de AP* [Policy response to a letter from the Dutch Personal Data Authority]. House of Representatives 2022-2023 26 64 no. 965

BZK (2024a). *Informatie- en communicatietechnologie (ICT)* [Information and Communication Technology (ICT)]. House of Representatives 2023–2024 26 643 no. 1149.

BZK (2024b). *Verzamelbrief Digitalisering juni 2024* [Digitalisation Letter, June 2024]. House of Representatives 2023-2024 26 643 no. 1197

BZK (2024c). *Evaluatie Rijksbreed Cloudbeleid* [Evaluation of central government cloud policy]. House of Representatives 2023-2024 26 643 no. 1225

Clingendael (2024a). *Too late to act? Europe's quest for cloud sovereignty.* The Hague: self-published

Clingendael (2024b). *Nederland en de EU: Zet in op cloudsoevereiniteit* [Netherlands and the EU. Pursuit of cloud sovereignty]. The Hague: self-published

CSR (2021). *Nederlandse Digitale Autonomie en Cybersecurity* [Dutch digital autonomy and cybersecurity]. CSR Advisory report 2021, no. 3

EZK (2023). *Agenda Digitale Open Strategische Autonomie* [Agenda, Digital open strategic autonomy]. House of Representatives, 2023-2024 reference 2023D42774

EZK (2024). *Antwoord op vragen van de leden Kathmann, Six Dijkstra en Sneller over de verhuizing van het.nl domein* [Answer to questions by MPs Kathmann, Six Dijkstra and Sneller on the relocation of the .nl domain]. House of Representatives 2023-2024 appendix 1305

Forum Standaardisatie (2024a). *Monitor Open Standaarden 2023* [Open standards monitor 2023]. The Hague: self-published

Forum Standaardisatie (2024b). *Standaarden en standaardisatieactiviteiten voor clouddiensten* [Standards and standardisation activities for cloud services]. The Hague: self-published

ICTU (2024). *Monitor Open Standaarden* [Open standards monitor]. The Hague: self-published

Moerel and Timmers (2020). *Reflecties over digitale soevereiniteit, Preadvies Staatsrechtconferentie 2020* [Reflections on digital sovereignty [Preliminary advice on constitutional law conference]. University of Utrecht: self-published

NCSC (2021). *(Publieke) clouddienstverlening: Enkele ervaringen uit onze cloud journey* [Public cloud services: some experience from our cloud journey]. The Hague: self-published

NCSC (2022). *Cloud Act requests (Memorandum of GreenbergTraurig to NCSC).* The Hague: self-published

Appendix 6 Endnotes

1. The CIBG is an agency of the Ministry of VWS. CIBG stands for Central Information Point for Healthcare Professions and was introduced in 2000. As the agency has assumed many more tasks since then that are not covered by the name, it now only uses the abbreviation CIBG.
2. We formalised these principles based on preliminary investigations and previous audits.
3. See for example: https://www.washingtonpost.com/national-security/2024/04/02/microsoft-cyber-china-hack-report/
4. See for example: https://nos.nl/artikel/2538710-datalek-bij-politie-hackers-bemachtigen-contactgegevens-alle-politiemedewerkers
5. See for example: https://ibestuur.nl/artikel/reddingspoging-franse-overheid-voor-atos-op-losse-schroeven/ and https://www.computable.nl/2024/10/08/onderhandelingen-tussen-franse-staat-en-atos-lopen-spaak/

6 Sources: https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft, https://www.dictu.nl/strategisch-leveranciersmanagement-oracle and https://www.rijksoverheid.nl/documenten/publicaties/2023/08/31/strategisch-leveranciersmanagement-rijk-voor-ibm-en-red-hat

7. https://www.dutchitchannel.nl/research/421377/google-en-microsoft-groeien-het-sterkst-in-public-cloud-markt
8. A cloud provided by a government service centre is a private cloud for the government as a whole. Our requests to the ministries and the summaries we received refer only to public, private and hybrid clouds.
9. See also: Netherlands Court of Audit (2024). Focus on AI in the Dutch central government. The Hague: self-published.
10. For a more detailed consideration of this term, we refer to recent reports by Clingendael (Clingendael, 2024a and 2024b).
11. This is a slightly amended definition proposed by Moerel and Timmers (2020).
12. Source: https://e-estonia.com/solutions/e-governance/data-embassy/

13 Sources: https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data, https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/#backingupgovernment

14. Sources: https://www.interxion.com, https://eur-lex.europa.eu, https://www.legalz.nl/blog/cloud-act, https://www.ncsc.nl/actueel/weblog/weblog/2022/de-werking-van-de-cloud-act-bij-dataopslag-in-europa, https://sosafe-awareness.com/blog/privacy-shield-decision, https://www.agconnect.nl/artikel/ec-neemt-nieuwe-privacyregels-aan-voor-datadoorgifte-aan-vs, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu
15. Source: https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu
16. See for example: https://www.dutchncca.nl/eu-cybersecurity-certification/cloud-services and https://ec.europa.eu/newsroom/cipr/items/713799/en
17. The Ministry of Defence is not subject to central government cloud policy. Certain aspects of the audit therefore do not apply to it.
18. We provided a template for this overview of cloud services. The characteristics we requested information on were: 1. Application/cloud service, 2. Service provider, 3. Cloud provider, 4. Reseller, 5. Contracts present?, 6. Service model (IaaS, PaaS, Saas) 7. General description of cloud services, 8. General description of cloud data, 9. Public, hybrid or private cloud 10. Material cloud usage? 11. Geographical region of processing and storage 12. Financial value of contract 13. Start date of contract 14. Expiry/end date of contract 15. Risk assessment made? 16. Did the assessment cover financial aspects (costs/benefits)?
    The exact request was for ‘an overview of all cloud contracts concluded for public, hybrid and private cloud services, both material and non-material cloud usage, for the ministry and organisational units such as agencies falling under the direct responsibility of the minister (but not autonomous administrative authorities).’.
19. Taken from Government I-strategy 2021-2025.
20. We analysed whether or not a strategic assessment of using the cloud had been facilitated and whether the method specifically considered the cloud. See also appendix 2 for our detailed control framework.
21. Namely 20 October 2022 regarding central government cloud policy and 26 June 2024 regarding government hardware and software procurement and contracting policy.
22. The name is no longer written out in full. See endnote 1.
23. See for example: https://www.washingtonpost.com/national-security/2024/04/02/microsoft-cyber-china-hack-report/
24. See for example: https://ibestuur.nl/artikel/reddingspoging-franse-overheid-voor-atos-op-losse-schroeven/ and https://www.computable.nl/2024/10/08/onderhandelingen-tussen-franse-staat-en-atos-lopen-spaak/

25. See for example: https://www.washingtonpost.com/national-security/2024/04/02/microsoft-cyber-china-hack-report/ and https://nos.nl/artikel/2538710-datalek-bij-politie-hackers-bemachtigen-contactgegevens-alle-politiemedewerkers

26. See appendix 1 for the specific contracts and agreements we examined for these 3 public cloud services.

27. Source: https://www.ssc-ict.nl/over-ssc-ict

28 The name is no longer written out in full. See endnote 1..

29 https://www.cibg.nl/onze-organisatie

30 See also the study commissioned by the Netherlands Standardisation Forum: Standards and standardisation activities for cloud services.

31. See for example: https://ibestuur.nl/artikel/reddingspoging-franse-overheid-voor-atos-op-losse-schroeven/ and https://www.computable.nl/2024/10/08/onderhandelingen-tussen-franse-staat-en-atos-lopen-spaak/

32. The name is no longer written out in full. See endnote 1.

33. We use the terms cloud services, applications, implementations, uses, systems, platform and services interchangeably. We also use the term cloud contract in reference to the above terms, specifically when they have been contracted.

This translation of the original Dutch text into English is provided by the Netherlands Court of Audit as a courtesy service. No rights can be derived from this translation. In the event of discrepancy between the Dutch original and the English translation, the Dutch original version shall prevail.

Netherlands Court of Audit
PO Box 20015
2500 EA The Hague
The Netherlands
+31 70 342 44 00
voorlichting@rekenkamer.nl
www.courtofaudit.nl

Original title
Het Rijk in de cloud; Donkere
wolken pakken samen

The Hague, January 2025