DIGITAL DEVELOPMENT PARTNERSHIP

Administered by WORLD BANK GROUP

GOVERNMENT MIGRATION TO CLOUD ECOSYSTEMS

Multiple Options, Significant Benefits, Manageable Risks

WITH SUPPORT FROM:

Google GSMA Microsoft

1818 H Street NW
Washington, DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

CONTENTS

Tables

Figures

Boxes

ACKNOWLEDGMENTS

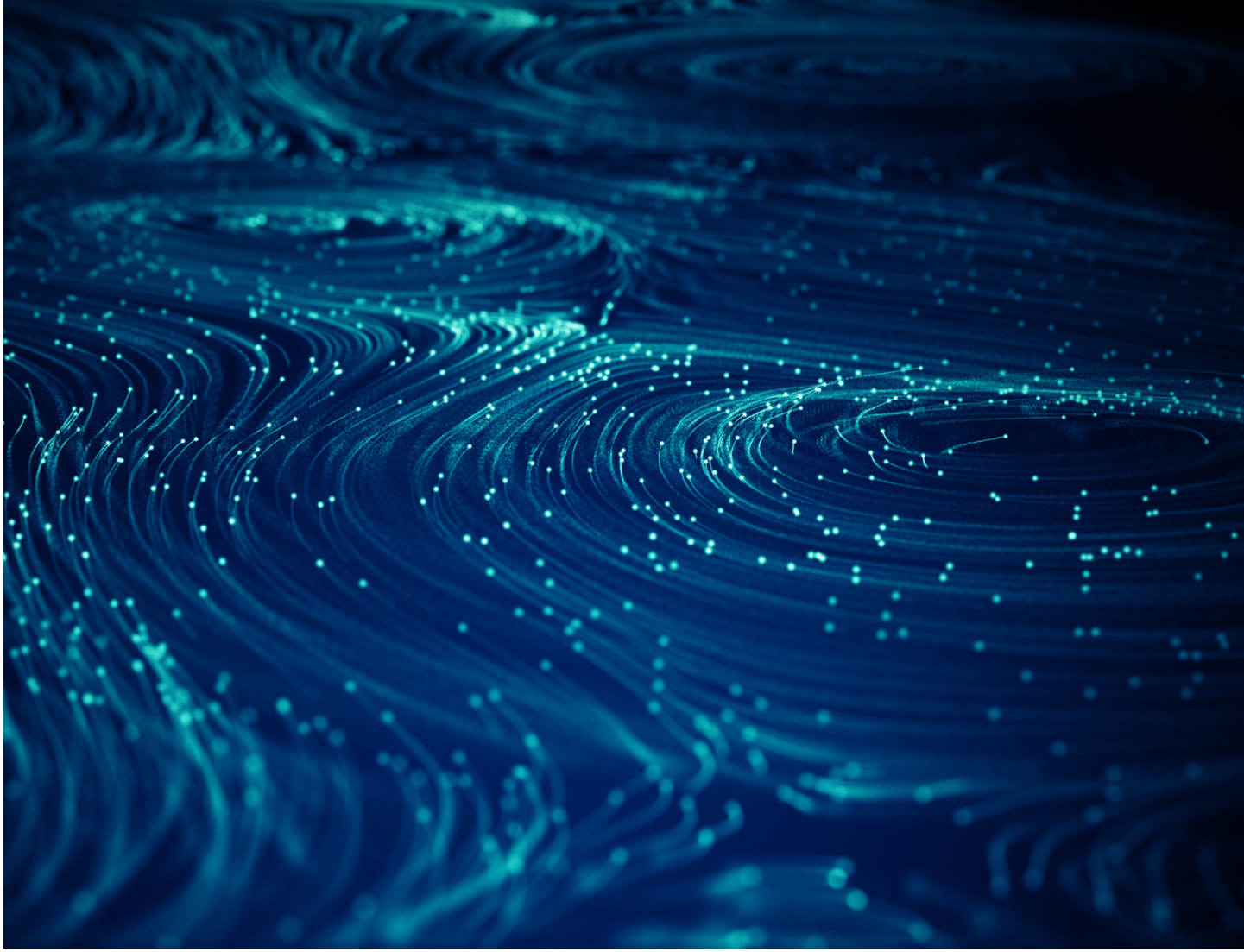
This World Bank report was authored by Rami Amin and Ed Hsu, under the leadership of Isabel Neto, Acting Practice Manager for the Global Knowledge Unit in the Digital Development Global Practice at The World Bank, and Christine Zhenwei Qiang, Director of the Digital Development Global Practice at The World Bank. This guide benefited from a background report produced by COWI, along with interviews, discussions, and comments from an Advisory Committee composed of cloud industry experts and thought leaders from Access Partnership, Amazon Web Services, the Asia Cloud Computing Association, Google, IBM, Microsoft, SAP, and Salesforce, as well as Equinix and PAIX. The authors would like to express gratitude for peer review comments received from across the World Bank Group for refining the message of the report, including from David Satola, Hunt La Cascia, Khuram Farooq, and Zaki Khoury from The World Bank, and Carlo Maria Rossotto and Ferdinand van Ingen from the International Finance Corporation (IFC). This report also benefited from the guidance of Natalija Gelvanovska-Garcia and Carlo Maria Rossotto, who together oversee the development of a forthcoming joint World Bank-IFC global report on cloud and data infrastructure. The authors are also grateful for editorial support from Steven Kennedy and Matthew Benjamin, as well as Takayo Muroga Fredericks for designing infographics used in this report, and Ping Ni for the overall design and cover page for this report.

This report was produced with generous funding support from the Digital Development Partnership (DDP), administered by the World Bank Group. The DDP offers a platform for digital innovation and development financing, bringing public and private sector partners together to advance digital solutions and drive digital transformation in developing countries.

Preface

This Report is a reference document to be consulted by governments, development partners, academics and others when considering, designing, implementing, or managing government use of cloud infrastructure and services.

This Report is based on evolving international good practice, as understood by the World Bank's Digital Development global practice. It reflects experiences in a range of countries from different regions, with different legal systems, and at different stages of economic development. It also takes into account existing literature, norms, and principles.



There is no guarantee that addressing all the issues raised in this Report will result in successful use of cloud services or infrastructure—that will depend on many factors that must be considered, and which may be different from country to country. While every attempt has been made to be complete, there may be issues affecting the design, establishment, or use of cloud services or infrastructure that are not addressed in this Report, or that are addressed in the context of certain assumptions, facts and circumstances that do not apply equally to every situation. This Guide is a reference tool only.

This Report is the part of a series that the World Bank Group will produce on cloud and data infrastructure. Forthcoming reports will focus on other themes, including the enabling ecosystem needed to facilitate cloud solutions, economic impacts of cloud infrastructure and adoption, the sustainability of cloud solutions and data centers, and legal and regulatory matters that affect the availability of cloud solutions and the design of cloud and data infrastructure within a country.

EXECUTIVE SUMMARY

Migrating from legacy IT infrastructure and data storage to cloud services can yield enormous benefits for governments: it can save governments money; increase the integrity, quality, and speed with which they deliver services; and provide access to the most advanced analytical tools and cybersecurity features available. These benefits have spurred a shift by governments across the globe away from legacy information technology (IT) systems, and towards cloud solutions, including public cloud services.

What is "the cloud"? While there are a few types of cloud architectures, the broadest definition is software, services, and applications – including storage – that are not hosted locally on a computer, requiring internet connectivity to facilitate computing. The cloud consists of private cloud providers, national or regional public cloud providers, and hyperscale cloud service providers. The private cloud is an option of cloud computing where data storage and processing infrastructure is used by only one organization or that ensures that an organization is completely isolated from others. Contrastingly, the national or regional public cloud provides some common services, such as storage and computing, but has only limited functionality and coverage. Strong local affiliation and knowledge allow regional public cloud providers to gain access where global players are not perceived as compliant. Hyperscale cloud computing consists of global players with a large catalogue of advanced services that can be offered to most countries. For governments, an ever-growing number of sophisticated software-as-a-service (SaaS) and platform-as-a-service (PaaS) business applications are available to solve specific public sector challenges through these public and private cloud solutions, such as registration, invoicing, and virtual team collaboration platforms, or more sophisticated applications such as customer relationship management, energy utilities, and sustainability dashboards to support green transitions.

This report helps governments identify considerations that may make one cloud option more suitable over another and provides guidance on how they can approach cloud migration decisions, as outlined in Figure ES.1. For example, the public cloud option is most suitable when a public sector entity seeks to increase cost efficiency without incurring upfront capital costs, when demand peaks are unpredictable, or when there is a need for advanced features such as artificial intelligence (AI)-enabled processing or enhanced cybersecurity. The private cloud may be more suitable for an entity that is governed by a restrictive regulatory framework, handles sensitive data, or can afford to continuously invest in high-performance technology and qualified information technology (IT) personnel. Most public sector entities will choose a hybrid cloud model that includes both public and private cloud services for different applications and requirements, reflecting the optimal tradeoff between costs, benefits, and risks. A variety of country-specific factors will further drive decision-making around the balance between public and private cloud options.

FIGURE ES.1 Comparison of benefits and challenges to consider between legacy on-premise data centers and different cloud options

	BENEFITS	CHALLENGES TO CONSIDER
DATA CENTER	• Strong data control that meets data-localization requirements	• Cost of maintaining and updating systems • Limited performance and capacity for quickly integrating the cutting-edge applications and innovation • Limited cybersecurity and more expensive to secure systems • Difficulty of building green data centers at small scale • High degree of internal technical expertise needed, including regular training costs
PRIVATE CLOUD		
ON-PREM	• Some cost savings if shared across government • Strong data control that meets data-localization requirements	• Cost of maintaining and updating systems • Limited cybersecurity and more expensive to secure systems • Difficulty of building green data centers at small scale • High degree of internal technical expertise needed, including regular training costs
OFF-PREM (HOSTED BY CLOUD SERVICE PROVIDER)	• Enhanced cost-efficiency • Potential cybersecurity and performance benefits and cost efficiency if provided by cloud service provider • Compliance with data-localization requirements	• Cost of maintaining and updating systems • Sustainability depends on cloud service provider • High degree of technical expertise required
PUBLIC CLOUD		
NATIONAL/ REGIONAL PUBLIC CLOUD PROVIDER	• Enhanced performance and scalability • Enhanced cost efficiency • Enhanced cybersecurity features • Compliance with data-localization requirements	• Often unclear or lower commitments to sustainability • Less control over data • Procurement will require close attention to service level agreements • Vendor lock-in
HYPERSCALE CLOUD PROVIDER	• Highest level of performance and scalability • Highest level of cost-effectiveness • Highest level of cybersecurity • Ability to quickly innovate due to access to most advanced tools, which can be more regularly updated • Strong commitment to sustainability through green data centers, use of renewable energy, and more efficient data management	• Procurement will require close attention to service level agreements • Potential vendor lock-in issues (though can be mitigated through multi-cloud solutions) • Data-localization and governance issues may limit this option

Governments across the globe are increasingly adopting public cloud solutions in particular for various reasons outlined in this report. The public cloud is a cost-effective way to use, maintain, and upgrade from on-premise (or on-prem) legacy IT infrastructure. It can help government institutions secure their databases and deploy cutting-edge cybersecurity mechanisms. It is efficient, resilient and reliable, and almost limitlessly scalable, as resources can be deployed on demand to meet institutions' changing needs. Public cloud computing also has the potential to significantly reduce energy and carbon emissions compared with other cloud options. While there are many benefits, it also introduces data, regulatory, technology, operational, vendor, and financial risks, which need to be governed and managed. Examples and lessons learned from other countries leading with migration to cloud services are provided in this report, along with further reference material.

This report is intended for governments and individual government entities considering moving their computational and data storage and processing functions to the cloud. As common with new technology, many will initially approach cloud migration – and indeed public cloud services – from a position of reluctance, viewing it as a risky proposition with limited benefits. This report aims to clear up misconceptions about the cloud, and in particular public cloud where there is often greater concern and confusion, as outlined in Table ES.1.

The second part of this report provides a three-level framework for government decision making to help navigate cloud options and facilitate cloud migration; this includes the policy, strategy, and operational-level considerations, as outlined in Figure ES.2

TABLE ES.1 Common misconceptions about the use of public cloud by Governments

MISCONCEPTION	REALITY
Use of the public cloud is costly.	Cloud computing is cost-efficient because it obviates or reduces the need to procure expensive equipment. Savings can represent 10–20 percent of the annual operating IT budget.
On-prem solutions are always more secure than the public cloud.	On-prem solutions are not inherently more secure, because most advanced security can be deployed in real-time when using cloud infrastructure.
The pace of innovation is the same when using public cloud and on-prem solutions.	Cloud services are better at fostering innovation because they are easy to use, can be quickly scaled, and provide new services as they become available, significantly reducing the time it takes to move from idea to working solution.
Public cloud solutions may not ensure data protection.	Public cloud entities are very different in nature from personal cloud products, such as Facebook. The business model of the public cloud fosters strong data protection. Technical steps can be taken to raise data protection to a very high level.
The cloud service provider (CSP) can see personal data and share it with a third party.	Nearly all CSPs encrypt data, meaning the data are not visible to the provider without decrypting. Most CSPs also support customer encryption keys, meaning that neither the CSP nor anyone else is able to view data without the customer-managed encryption key.
Cloud solutions are difficult to scale.	Cloud services have a nearly unlimited scalability (so-called cloud elasticity). They therefore allow governments and other public entities to scale up during times of high user demand, such as during a pandemic like Covid-19.
Cloud solutions are less sustainable than legacy systems.	Use of cloud computing can reduce energy consumption and carbon emissions by up to 30 percent, because of economies of scale.
All types of clouds are equal.	For larger data migration needs, a public hyperscale cloud is usually the optimal path for achieving the full benefits of the public cloud, because of the depth and breadth of services offered.
On-prem infrastructure needs to be developed before moving onto the cloud.	No on-prem infrastructure is needed to start using cloud services, illustrating one of the most critical value-propositions of cloud services – particularly in low-IT capacity settings.
Cloud solutions require advanced, high-speed connectivity.	Developments in technology and low-powered Internet of Things (IoT) devices, as well as containerization allow public agencies to deploy solutions even where connectivity is low. Some hyperscale cloud providers offer specialized services for low-connectivity clients.
Getting started requires a large investment.	The public cloud allows organizations to start with small and simple use-cases and scale later if the solution works as intended. No significant up-front capital investment is needed.

FIGURE ES.2 Three step framework for navigating cloud migration options

- The **policy level** defines the vision for migrating to the cloud, based on objectives to be achieved. It determines the optimal mix of private and public cloud services. The framework suggests that there is a "mature state" that allows a given country or government entity to derive the maximum possible cost-effective benefits from the public cloud, where they are available.
- The **strategy level** identifies the domains that lend themselves most readily to cloud solutions. A clear system for data classification is essential to identifying which types of data can be moved to the public cloud and who the main stakeholders are.
- The **operational level** focuses on the practical details of putting public cloud projects into operation. It includes identifying the core challenges facing public sector entities that are starting their cloud migration process, such as vendor lock-in. The report describes in broadstrokes a process for initiating a public cloud project, including steps for estimating the operational expenses and cost savings, and signing a service level agreement (SLA).

This report is the first in a series that the World Bank Group will produce on cloud and data infrastructure. Forthcoming reports will focus on other themes, including the enabling ecosystem needed to facilitate cloud solutions, economic impacts of cloud migration, the sustainability of cloud solutions and data centers, and legal and regulatory matters that affect the availability of cloud services and the design of local cloud and data infrastructure. All of these reports are directed towards governments, policymakers, and other development stakeholders who are positioned to facilitate the broader cloud and data infrastructure agenda in developing countries and emerging markets.

1. INTRODUCTION

The COVID-19 pandemic demonstrated the importance of digitalization of government services, as countries that had invested in these technologies were better able to adapt to the crisis and showed greater resiliency than countries that had not. This has included the ability for civil servants to transition to remote work, the online delivery of existing and new benefits, the use of data to manage supply chains and target interventions and support, and the continued operation of parliaments and courts. The virtualization of these processes that can be facilitated by cloud computing technology and services demonstrates another critical step in the digital development pathway for governments. Indeed, cloud services can help governments provide better health care, education, social amenities, justice, and public safety, and can also help governments harness other emerging technologies such as artificial intelligence (AI), distributed ledger technology, and blockchain. Examples of specific government applications include:

- making unemployment, retirement, death, and childbirth payments automatically
- improving the provision of social insurance
- classifying emergency calls based on their urgency
- building scalable and user-friendly education systems that can handle student enrollment
- predicting the spread of infectious diseases
- identifying fraudulent benefit claims and tax evasion patterns
- anticipating road maintenance requirements
- assisting with defense and national security military simulations.

Cloud technologies can also save governments money; increase the integrity, quality, and speed with which they deliver services; and provide access to the most advanced analytical tools and cybersecurity features available. These benefits have spurred a shift by governments across the globe away from legacy information technology (IT) systems, and towards cloud solutions, including public cloud services. As seen with previous technology deployments, government adoption of cloud services has been uneven across the Global South, contributing to a further widening of global digital divides. While some governments have taken an early lead, such as the UK, Australia, and Singapore, there remain many where there is a lack of clarity around what the cloud is, how it's different, and how it can support different applications and use cases given unique national characteristics and regulations.

Box 1.1

WHAT IS "THE CLOUD"?

The cloud consists of private cloud providers, national or regional public cloud providers, and hyperscale cloud providers, which provide on-demand data storage and processing services accessed through the internet, which may use computing infrastructure that is stored on or off premise.

- The **private cloud** is a form of cloud computing where cloud hardware is provided and/or operated by cloud providers and used by only that organization or that ensures that the organization's data is completely isolated from others.
- The **national or regional public cloud** provides some common services, such as storage and computing, but it has only limited functionality and coverage. Strong local affiliation and knowledge allow regional public cloud providers to gain access where global players are not available, or not perceived as compliant with national regulations.
- The **hyperscale cloud** consists of global players with a large catalogue of advanced services that can be offered to almost all countries.

Sources: https://www.gartner.com/en/information-technology/glossary/private-cloud-computing; https://www.srgresearch.com/research/hyperscale-cloud-market; https://www.accenture.com/_acnmedia/PDF-143/Accenture-Hyperscale-Cloud-Journey.pdf#zoom=40.

Government spending on public cloud services is estimated to have grown by 17.1 percent between 2020 and 2021[1], and further estimated to reach nearly $500 billion amongst end-user spending in 2022, and $600 billion by 2023.[2] Almost half of government organizations worldwide are now using cloud services. Local governments spent 20.6 percent of their IT budgets on cloud services, and national governments spent 22.0 percent.[3] By 2026, global public cloud spending is projected to exceed 45 percent of all enterprise IT spending, up from less than 17 percent in 2021.[4]

Digitizing public services – even without cloud solutions – has long been demonstrated to enable governments to become more efficient and resilient, allowing them to improve the quality of the services they provide citizens. Advantages of digitalized public services include the following (Daub et al. 2020):

[1] https://www.gartner.com/smarterwithgartner/understanding-cloud-adoption-in-government.

[2] https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022

[3] https://www.gartner.com/smarterwithgartner/understanding-cloud-adoption-in-government.

[4] https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud.

- 24/7 accessibility of governmental services
- a 50 percent reduction in the time citizens spend interacting with public administration
- a 50 percent reduction in the costs companies incur interacting with the public administration
- a 60 percent reduction in government case-handling efforts.

While these advantages from digitalization could be achieved without the use of cloud technology, doing so would take longer to set-up, be more difficult to scale, limit access to the most advanced data analytics tools, and require significantly larger capital investments and internal resources and expertise to manage.

Despite the enormous benefits of cloud technology, many developing countries have been slow to adopt it. Cloud-related activities in the developing world remain concentrated in large and more developed economies in the Global South, such as China, India, Brazil, South Africa, and Vietnam, although the cloud is gradually making inroads in smaller and less developed economies. A growing diversification of data center locations and a widening array of entrants offering cloud services are now creating roles for enterprises and governments in emerging economies. Increasingly, governments are collaborating with domestic and foreign players to develop new digital products that serve local needs. This activity creates opportunities on the supply side, as information and communications technology (ICT) companies and mobile operators can leverage existing infrastructure to deliver cloud services, diversifying their revenue streams and growing their bottom line. The business potential of mobile operators is high in developing countries in particular, where penetration of mobile phones is greater than that of personal computers, creating natural opportunities for mobile-based cloud computing and integration with public service delivery.

The purpose of this report is to help policy makers, government officials, teams from the World Bank and other development finance banks, and other development stakeholders understand how governments can harness the benefits and manage the risks of adopting new cloud services to improve government service delivery. The report is structured as follows:

- Section 2 describes differences between various private and public cloud services
- Section 3 describes the benefits and challenges to consider with adopting cloud solutions
- Section 4 presents different options governments have for cloud migration and adoption
- Section 5 presents a decision-framework for governments to consider at the policy, strategy, and operational levels to help them navigate different migration options

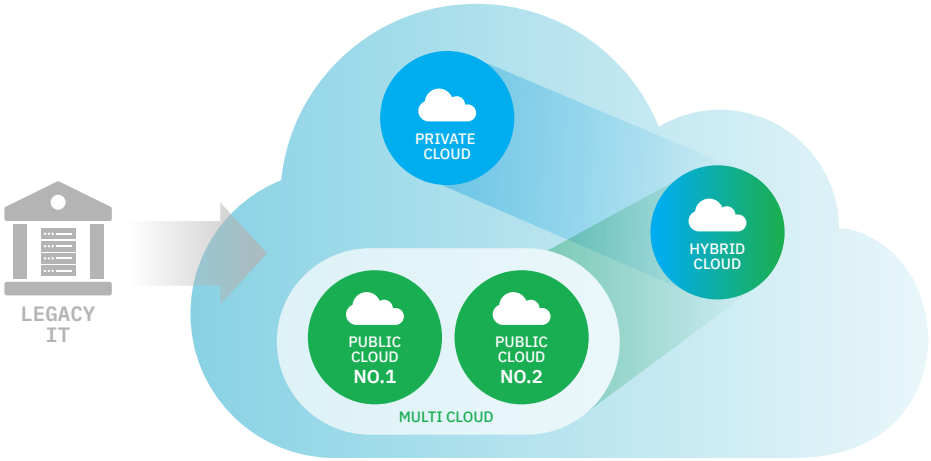
The target audience for this report is public sector decision makers with an interest in advancing the digital development agenda and connecting to – and benefitting from – the global digital economy. This report is intended for officials at both the government-as-a-whole and the individual agency level. This expanded scope reflects that fact that public cloud projects need not be driven by government-wide initiatives but can be initiated with narrowly focused investments by single agencies looking to solve a concrete challenge.

This guide is part of a series that the World Bank Group will produce and disseminate on the broader cloud and data infrastructure agenda. Forthcoming reports will focus on other cloud services and infrastructure themes, including the enabling ecosystem needed to facilitate cloud solutions, economic impact of cloud migration, the sustainability of cloud solutions and data centers, and legal and regulatory matters that are critical to deciding among cloud service options, such as data sovereignty rules and requirements.

2. DIFFERENT CLOUD SERVICE MODELS

When transitioning from legacy IT infrastructure systems for data storage and processing, governments may opt to use a private cloud, a public cloud, a multi-cloud model, or a hybrid solution that combines and interconnects the two different types of cloud services (with or without storing data externally), as illustrated in Figure 2.1.

FIGURE 2.1 Different Cloud Service Models



A private, on-premise cloud solution is similar in many respects to a traditional data center, but with additional layers to facilitate virtualization and cloud services on-site. The customer is responsible for everything from the infrastructure layer (servers, data storage units, networks) to the platforms and software. It is analogous to owning a car and being responsible for everything from operation to maintenance.

The private cloud essentially provides software services that traditional data centers do not. These services include virtualization and cloud orchestration software that is used for automation, management, and monitoring. Governments can choose to operate a private cloud themselves, or they can use an external private cloud provider. The private cloud can be housed at a government-owned facility or located off premises at a private cloud facility. Private cloud options generally provide access to only a subset of cloud services, although they can provide more direct control of the hardware.

In a private, off-premise solution, a cloud service provider is responsible for providing (hosting) the infrastructure, but that infrastructure is dedicated to one customer exclusively. The customer – a government entity for the purpose of this guide – is typically responsible for the platform and software layers. While the provider may provide infrastructure to other customers, each customer's infrastructure is kept separate. The situation is analogous to renting a car: the rental customer does not own the car but has sole control over it and is responsible for insuring it, fueling it, and driving it.

Contrastingly, public clouds are owned and operated by cloud service providers which assume all responsibility for the data centers, hardware, and infrastructure on which customer workloads run. They are delivered and accessible via the Internet and often provide web-based email, online office applications, storage, and other services.[5] The public cloud maximizes the benefits of a low-cost structure and rapid capacity increases. An overview of public and private cloud options is outlined in Table 2.1 using car transport options as a conceptual analogy.

TABLE 2.1 Options for delivering cloud services

	ON-PREM	OFF-PREM
Private Cloud	You are responsible for everything from the infrastructure layer (i.e., servers, storage, and networking) to the platforms and software *Analogy: This is like owning a car where you are responsible for everything from operation to maintenance*	A Cloud Service Provider (CSP) is responsible for providing (or hosting) the infrastructure, but it is dedicated only to you. You are typically responsible for the platform and SW layers on top of the infrastructure layers to other customers, but they are separate from each other. *Analogy: This is like leasing a car in which you don't own the car, but it's dedicated to you, and you are responsible for insurance, gas and driving it.*
Public Cloud	Not A Valid Option	This is an on-demand public utility where CSP (e.g., Google, AWS, and Azure) is responsible for the infrastructure, platform and software services it provides, and you only pay for what you use *Analogy: This is like using a taxi service in which you are not responsible for any aspect of the service other than just using the service.*

Governments choosing a hybrid option may elect to store their data at an on-prem data center and use a public cloud only to process workloads. Or they may use a virtual private network (VPN) to connect to a public cloud. While private cloud services permit on-premise hosting of IT infrastructure (servers, data storage units, networks), platforms, and software, public clouds do not. Both private and public clouds can provide off-premise (remote) hosting of the same mix of assets.

[5] https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/.

The data center infrastructure that supports public cloud services are off-premise, and a variety of factors determine optimal location of these data centers including distance to customers, broadband connectivity infrastructure, climate conditions, and access to reliable energy sources (and increasingly – particularly in the case of hyperscale data centers – access to renewable energy). Public cloud service providers functions as an on-demand public utility, responsible for all the services it provides (infrastructure, platform, software). Customers pay only for what they use. The analogy is a taxi or ride service: the customer is responsible only for paying the fare, while the rest of the costs are the responsibility of the taxi or ride service provider. The benefits and challenges to consider regarding traditional data centers, private clouds, and public cloud services are summarized in Figure 2.2.

Providers of cloud-based computing services are a diverse group of companies that offer distributed computing. The market has evolved rapidly since the inception of modern cloud computing in the early 2000s.[6] Public cloud providers vary along two dimensions: breadth of services and depth of services.

Breadth of services refers to the number of services a provider offers. The largest public cloud providers (Google, Microsoft Azure, AWS, Alibaba, and a few others), which are referred to as 'hyperscalers' due to their ability to offer the greatest range of horizontal scaling for services, offer the broadest range of services and the most advanced technical capabilities. Their services include a wide range of out-of-the-box machine learning products, such as chatbots with natural language processing and image-recognition services.[7] Each of the hyperscalers is increasingly growing services that are focused on government needs and requirements for managing data, especially through dedicated software solutions delivered over the cloud. These services allow public sector entities to quickly deliver better services to citizens following a migration to the cloud. For example, a local government can deploy a chatbot to interact directly with citizens, without the significant upfront investment that would otherwise be required.[8]

Depth of services refers to the number of features a cloud service has. Hyperscale cloud providers compete to develop their services to offer products that are superior to those provided by other providers – whether other hyperscalers, or smaller, more local service providers. They can offer graphical processing units for use in training machine learning models or high-performance computing, which smaller public cloud providers cannot. In addition, hyperscale cloud providers are able to enhance their services based on the experiences of their clients in solving real-world challenges. On the more advanced end, hyperscale cloud providers can even facilitate quantum computing in the cloud, a cutting-edge technology that requires extensive research and development to implement, which smaller players are not positioned to offer.[9]

---

[6] https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/.

[7] https://www.uxmatters.com/mt/archives/2018/02/the-opportunities-of-cloud-computing.php.

[8] https://cloud.google.com/customers/placer-county.

[9] https://research.aimultiple.com/quantum-computing-cloud/.

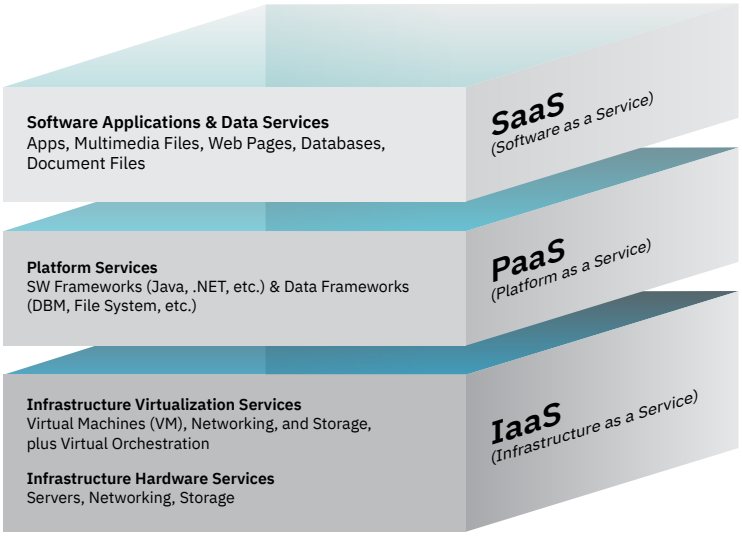
FIGURE 2.2 Comparison of benefits and challenges to consider for traditional, legacy on-prem data centers, private clouds, and public clouds

	BENEFITS	CHALLENGES TO CONSIDER
DATA CENTER 	• Strong data control that meets data-localization requirements	• Cost of maintaining and updating systems • Limited performance and capacity for quickly integrating the cutting-edge applications and innovation • Limited cybersecurity and more expensive to secure systems • Difficulty of building green data centers at small scale • High degree of internal technical expertise needed, including regular training costs
PRIVATE CLOUD		
ON-PREM 	• Some cost savings if shared across government • Strong data control that meets data-localization requirements	• Cost of maintaining and updating systems • Limited cybersecurity and more expensive to secure systems • Difficulty of building green data centers at small scale • High degree of internal technical expertise needed, including regular training costs
OFF-PREM (HOSTED BY CLOUD SERVICE PROVIDER) 	• Enhanced cost-efficiency • Potential cybersecurity and performance benefits and cost efficiency if provided by cloud service provider • Compliance with data-localization requirements	• Cost of maintaining and updating systems • Sustainability depends on cloud service provider • High degree of technical expertise required
PUBLIC CLOUD		
NATIONAL/ REGIONAL PUBLIC CLOUD PROVIDER 	• Enhanced performance and scalability • Enhanced cost efficiency • Enhanced cybersecurity features • Compliance with data-localization requirements	• Often unclear or lower commitments to sustainability • Less control over data • Procurement will require close attention to service level agreements • Vendor lock-in
HYPERSCALE CLOUD PROVIDER 	• Highest level of performance and scalability • Highest level of cost-effectiveness • Highest level of cybersecurity • Ability to quickly innovate due to access to most advanced tools, which can be more regularly updated • Strong commitment to sustainability through green data centers, use of renewable energy, and more efficient data management	• Procurement will require close attention to service level agreements • Potential vendor lock-in issues (though can be mitigated through multi-cloud solutions) • Data-localization and governance issues may limit this option

The benefits of the public cloud depend on the type of provider chosen. Private cloud options generally provide access to only a subset of cloud services and hence provide only limited benefits, although they can provide more direct control of the hardware. Regional or local public cloud providers also provide only a subset of the hyperscale benefits, although they do so through local connectivity, which can be desirable or indeed required under national data localization rules, a feature manifest in many developing countries, limiting access to hyperscale service providers.

The cloud provides services at varying levels of customization (Figure 2.3). The top layer, software as a service (SaaS), represents the most "packaged" solution. For these services, the cloud provider manages nearly all aspects of the digital solution. At the other end of the spectrum lies infrastructure as a service (IaaS). In this kind of service, the client retains full control of the solution's configuration. In between, platform as a service (PaaS) includes infrastructure, along with another layer of development tools and applications to enable the customer to design their own applications to suit purpose. Ideally, SaaS, PaaS and IaaS solutions should address the precise need faced by the public agency – and last section of this guide will provide some guidance on how to approach this. Where the match between the service and the need is not perfect, some customization or self-developed applications will be needed on top of the public cloud infrastructure, which PaaS can enable. All of these service models include the standard benefits associated with cloud solutions that have been mentioned throughout this report, including cost efficiency and ability to rapidly scale services as needed.

FIGURE 2.3 Services provided at each layer of the cloud



Source: World Bank 2021.

A competitive vendor selection process can help public entities determine which cloud provider is the best fit for a particular use case, and ongoing work at the World Bank is focused on developing a more robust framework for governments. Governments can also consider using third-party accreditations or industry standards to drive decision-making with procurement, such as those provided in Appendix A.

3. BENEFITS AND RISKS OF MIGRATING TO CLOUD SERVICES

Migrating to the cloud – and public cloud services in particular – brings multiple benefits for governments and ministries, improving cost efficiency, data security, performance enhancement, scalability, and innovation. It can enhance the quality of public services and have positive impacts on environmental sustainability. Governments, ministries, and other public entities that are behind in their transition to cloud services are missing out on the multifaceted benefits that cloud computing can provide. These countries will fall further behind in the global digital divide if they do not adopt cloud solutions where they make sense given resources available, application needs, and local contexts. But cloud solutions also entail risks, which governments and ministries need to assess before initiating their transition. This section describes both key benefits and risks most cited from the experience of other countries that have already begun making the transition to cloud services, outlining important considerations for government decision-makers around costs, security, data protection, performance and reliability, and finally, environmental sustainability. The subsequent chapter will consider these benefits and risks within the context of different cloud migration options available.

Cost

Cloud computing is a cost-effective way of using, maintaining, and upgrading from on-prem legacy IT infrastructure. Cost savings are achieved by obviating the need to procure expensive server equipment, desktops, and licenses, which require significant time and labor to set up and maintain. These savings can represent 10–20 percent of annual IT budgets (KPMG 2014). Among the cost saving benefits of using the cloud are the following:

- no upfront hardware and software purchases (CAPEX)
- reduced spending on computing, storage, networking, and security
- reductions in operational, maintenance, replacement, and upgrade expenses, including need for operations-oriented personnel
- increased productivity
- ability to scale dynamically with load, optimizing the use of capacity.

Box 3.1

UNLOCKING THE POTENTIAL OF THE PUBLIC CLOUD AT ISRAEL'S MINISTRY OF TOURISM

The Israeli Ministry of Tourism was the first Israeli ministry to transition to the public cloud, migrating in 2015. It decided to integrate a Microsoft 365 infrastructure at its many overseas offices, which conduct marketing activities to attract tourists to Israel. This infrastructure provided e-mail, calendar, and file-sharing services, which replaced local mail services. The main reasons for migrating were to increase the quality of services abroad, eliminate the need for multiple servers, and reduce the costs of providing complex and expensive technical support for these services.

During the COVID-19 pandemic, Israel gradually removed some of the legal barriers that had prohibited government ministries and other public entities from uploading information to the cloud. The change has allowed the Ministry of Tourism to conduct full audit processes using a tablet application. Other processes—such as procurement and management relations with the local tourist industry—are expected to transition to the cloud.

Sources: https://www.pc.co.il/news/202038/; https://www.pc.co.il/news/315660/.

The scalability of cloud services implies that users no longer need to lose out from over-provisioning or under-provisioning hardware, which can be difficult to predict at time of procurement.

Israel's ministry of tourism provides a good example of how migration to public cloud solutions can yield cost savings (Box 3.1).

Security

Among cloud options, the public cloud – and in particular hyperscale public cloud service providers – can help government institutions increase cybersecurity by deploying cutting-edge defense mechanisms. Doing so is critical because the rapidly growing sophistication of tools with malicious intent (Malwarebytes Lab 2020) has made it easier than ever to damage a government's digital infrastructure (Kaloudi and Li 2020). Cryptography attacks (commonly known as ransomware) have become increasingly common (Al-rimy, Maarof, and Shaid 2018). Growing security threats have forced organizations to continuously improve and upgrade their IT security technology and standards to keep up with the changing threat landscape. Digital government infrastructure are especially common targets for attack, with developing countries particularly at risk due to the lower cybersecurity capacity and personnel.

Use of the public cloud – and hyperscaler service providers in particular – allows governments to apply sophisticated technology—such as stringent identity access management and multi-factor authentication encryption at rest and in transit—that would be very costly to acquire on their own. Handling tasks such as comprehensive auditing and enforcing the principle of least privilege (which dictates that a user should be granted the lowest possible level of privileges needed to complete a specific task) are very difficult unless strong security capacities are in place, and these capabilities must be continuously updated to be able to respond to new security threats.

Cloud providers invest heavily in keeping security features up to date to match attackers' capabilities and constantly develop new security features, such as threat detection based on machine learning.[10] They can quickly apply patches, and isolate parts of customer's assigned infrastructure as needed. Using public cloud providers also allows government entities to rely on a security framework developed by highly trained engineers without having to make their own massive investments in security – including both hardware and staff (NCSC 2020; Rawat, Singhal, and Choudhury 2021).

Almost all cases of security breaches are caused by users' mismanagement of the controls designed to protect their data, not the cloud provider's failure to deploy adequate safeguards. Consequently, it is important for governments and ministries to develop appropriate cloud strategies and policies before migrating data and to assign a management team to monitor their implementation.[11] Additionally, security is a 'shared responsibility' between cloud customers and vendors, and so even going with a hyperscale provider does not fully relieve a government entity – or any entity – of the critical need for internal cybersecurity capacity.

Data protection

Cloud services can provide a high level of protection for sensitive data by preventing the unauthorized identification of data stored on the cloud. To protect and secure their data in cloud environments, governments must know what data they have and where those data are located; what types or classes of data are exposed, how they are exposed, and what the potential risks are; and which applications are being accessed, by whom, and for what purposes. However, more than half of IT practitioners do not know where sensitive or confidential data are located. Not knowing where data are stored makes it difficult to know who can access them (Ponemon Institute 2014).

Personal cloud computing does not treat data protection in the way that the public cloud services do, because of former's use of data profiling, as well as business models that monetize user data to increase advertising revenue. Hyperscale cloud

[10] https://docs.microsoft.com/en-us/azure/security/fundamentals/threat-detection.

[11] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure.

providers do neither; instead, they charge a fee for each cloud service they supply. Generally public cloud providers apply the following practices to protect user data, sharing some of the responsibility with users:

- Users, not the provider, control data; the cloud provider processes the data according to a service level agreement specifying the services and guarantees it will supply. Many companies enable flexibility in the design of these services to suit customer needs – which will be different for each government entity.
- Advertisements targeting users are not permitted, and data are never sold to third parties.
- Data collection and use are transparent, complying with regulations such as the European Union's General Data Protection Regulation (GDPR),[12] Australia's Privacy Act,[13] Brazil's Lei Geral de Proteção de Dados,[14] the California Consumer Privacy Act,[15] Canada's Personal Information Protection and Electronic Documents Act,[16] or Japan's Personal Information Protection Commission.[17]

Data-protection requirements are country-specific and depend on national and local laws. Some countries mandate that certain types of data must be kept within a certain jurisdiction while other types may reside on the public cloud, transmitted through data centers located beyond national borders. Data-localization requirements can reduce the security of data in lower-capacity settings (Wu 2021), and consequently they cannot always facilitate the most effective security measure. Governments need to be aware of these laws before they take steps to migrate their data to the cloud. Forthcoming reports by the World Bank will examine additional legal issues, including implications of legislation such as the U.S. Cloud Act, which are beyond the scope of this guide.

Public cloud providers encrypt data with an encryption key that they hold. Encryption and decryption can be handled in three ways[18]:

- In customer-managed encryption, users encrypt their data with encryption and decryption keys provided and managed by the cloud platform. The cloud provider holds the decryption keys.
- In customer-supplied encryption, the public cloud platform stores only the encryption key. The customer holds and manages the decryption keys.
- In client-side encryption, the customer handles all encryption and decryption; the cloud platform does not store any keys.

12 https://cloud.google.com/security/gdpr.
13 https://cloud.google.com/security/compliance/australian-privacy-principles.
14 https://cloud.google.com/security/compliance/lgpd.
15 https://cloud.google.com/security/compliance/ccpa.
16 https://cloud.google.com/security/compliance/pipeda.
17 https://cloud.google.com/security/compliance/ppc-japan.
18 https://turbulentflux.com/data-security-public-cloud-platform/.

Institutions that rely on multiple cloud service providers – a fairly common phenomenon among government cloud ecosystems – may have little or no control over the movement of their data through different data centers around the world (Deloitte n.d.). In addition, it is not always clear whether the data custodian or the third-party service provider is responsible for protecting data or which sets of data-protection laws apply. Cloud service providers may also be reluctant to fully disclose the security measures they use to protect information or how they process the data. This puts the onus on governments to ensure cloud service providers meet any local data protection needs and statutory requirements during the review of service-level agreements, and particularly within the context of any legal or regulatory changes within a country that may transpire after a contract is signed.

Performance and reliability

The primary indicator of reliability for cloud services is uptime—the percentage of time a server operates. On-prem systems appear to have virtually 100 percent uptime. But running an application 24/7 on-prem is less efficient than public cloud solutions, which have better optimization options, can scale to actual demand, and provide extensive fallback measures in case of disaster or system outage. The improved utilization rate of hyperscale public cloud service providers has the added benefit of also yielding overall savings in energy consumption, as will be discussed later in this section.

Most public cloud providers have extensive disaster recovery procedures that they constantly improve to keep them resilient to both physical and cyber risks, with hyperscale cloud providers having many layers of redundancy. At Amazon Web Services (AWS), for example, multiple data centers cover the same region, so that service is provided even if a natural or man-made disaster affects one center. AWS continuously replicates both data and applications and has backups that allow for continuous operation and extremely limited downtime.[19] Other competing hyperscale cloud providers have similar levels of performance and reliability.

Cloud performance metrics monitor resources to ensure that all components communicate seamlessly. These metrics measure input/output operations per second, file system performance, reachability, and autoscaling. In principle, a government-hosted data center could provide these features and conduct this kind of monitoring, but doing so would be prohibitively expensive, losing out on cost efficiency at scale that hyperscale cloud service providers benefit from.

[19] https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html; https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/.

Scalability

Scalability refers to how well a system can react and adapt to changing demands. The cloud – particularly hyperscale public cloud – provides near-unlimited scalability, by allowing users to:

- Add and drop services on demand. This "cloud elasticity" can be automatic and seamless.
- Build a system with additional components (by, for example, linking a server to others to add processing power or memory). This "horizontal scaling" can increase redundancy and ensure that services remain available and reliable.
- Manage different types of scaling automatically (autoscaling). This ability to scale seamlessly is extremely useful in handling normal peak loads (such as school enrollment) and reacting to emergencies (such as natural disasters or pandemics). In Australia, for example, cloud-based infrastructure allowed the government to scale its systems to handle both reporting of wildfires and the impact of COVID-19 (SAP 2020).

Environmental sustainability

Cloud computing can also reduce government energy consumption and carbon emissions by a net 30 percent or more compared with running the same applications on their own infrastructure,[20] because cloud providers benefit from economies of scale, particularly public hyperscale cloud providers. The benefits are especially large for small institutions, which can enjoy net energy and carbon savings of more than 90 percent.[21]

Four factors have allowed data centers to keep their energy usage stable despite an increase in data center workloads and Internet traffic (IEA 2021). The factors are (1) IT operational efficiency; (2) IT equipment efficiency; (3) efficiency of data center infrastructure; and (4) electricity generated from renewable sources. Each factor is described below.

Operational efficiency of large cloud providers is high because of three factors:

- Dynamic provisioning: Large operations enable better matching of server capacity to demand on an ongoing basis.
- Multitenancy: Large public cloud environments can serve millions of users and thousands of companies simultaneously on one massive, shared infrastructure.
- Server utilization: Higher equipment utilization rates mean the same amount of work can be done with fewer servers, which in turn leads to less electricity consumed per unit of output.

---

[20] https://news.microsoft.com/2010/11/04/microsoft-accenture-and-wsp-environment-energy-study-shows-significant-energy-and-carbon-emissions-reduction-potential-from-cloud-computing/.

[21] A 2018 study finds that the Microsoft cloud is as much as 93 percent more energy efficient and as much as 98 percent more carbon efficient than on-prem solutions.

- IT equipment efficiency is the second factor. It is generally high with public cloud providers because these companies spend a significant portion of their operating expenses on electricity to run IT equipment—much more than the typical corporate IT department. Therefore, they have strong financial incentives to optimize efficiency.

Third, large data centers – particularly hyperscaler cloud service providers, use advanced technologies that reduce electricity requirements for overhead tasks such as lighting, cooling, and power consumption. Power usage effectiveness (PUE)—the ratio of overall electricity consumption at the data center facility to the electricity delivered to the IT hardware—is a common measurement of how efficiently a data center uses electricity. The hyperscale data centers that power the cloud achieve much greater PUE than on-prem data centers. Through innovation and continuous improvement, the cloud providers lead in designing, building, and operating data centers that minimize energy use for a given amount of computing power.

The fourth factor is energy from renewable sources. Consolidating distributed electricity demand from on-prem data centers unlocks the potential for large-scale purchases of green power that bring substantial renewable energy projects onto the grid that were not otherwise viable. The levelized costs of renewables such as wind and solar have decreased significantly in recent years, making renewables the cheapest source of energy available on the grid in some areas. IT companies consume electricity from the regional electricity grids, but by signing power purchase agreements with, for example, wind and solar project developers, they can draw additional renewable energy into the grid system. This energy is either purchased directly from renewable developers or secured through partnerships with utilities. To ensure that their energy procurement has a meaningful environmental impact, companies must apply strict standards of “additionality,” ensuring that all renewable energy purchases bring new renewable energy capacity onto the grids where they operate. Box 3.2 provides examples of efforts by one hyperscale cloud service provider, Google Cloud, to increase the use of renewable energy in computing.

Box 3.2

GOOGLE CLOUD'S COMMITMENT TO – AND PROCUREMENT OF – RENEWABLE ENERGY

When Google purchases renewable energy, it applies the following principles:

- **Additionality.** Google signs agreements with projects before construction, ensuring that its purchases lead to carbon reductions by displacing carbon-emitting generation on the grids where they operate.
- **Bundled physical energy.** Google purchases both the physical renewable energy and the corresponding renewable energy certificates (RECs) or guarantees of origin (GOs) in Europe. Doing so ensures that Google provides all or nearly all the project's cash flow over time, as opposed to purchasing only the REC or GO, which provides a small portion of the project's cash flow.
- **Proximity.** Where possible, Google purchases renewable energy from projects that will operate on the same grids as its data centers so as to forge a stronger link between the renewable power that Google purchases and its data center consumption.

Google procures renewable energy in four ways:

1. Direct renewable purchasing. Deregulated wholesale and retail power markets make it possible for Google to directly purchase renewable energy and have it contractually delivered to data centers consuming electricity on the same regional grid. Building onsite self-generation facilities is another approach.

2. Fixed-floating swaps. In areas where it is not possible for renewable energy to be contractually delivered to the data center, Google can still sign a power purchase agreement (PPA) known as a fixed-floating swap. Under this structure, Google signs a PPA for renewable electricity and obtains the RECs or GOs with the project developer, which then sells renewable electricity from the project on the wholesale market.

3. Utility renewable energy tariffs. In areas where retail markets are not open to competitive suppliers, particularly where there is no auction-based wholesale market, Google works with utility providers to create a new rate class called a "renewable energy tariff" (also known as a "sleeved PPA" structure), in which the utility procures renewable energy (either through a PPA or asset ownership) for sale and delivery to Google's data center.

4. Grid-mix renewable content. The utility's grid mix contains energy from renewable resources that is not otherwise being purchased by specific consumers and is part of the "residual" mix. For each MWh of retail electricity consumed by a Google data center, the company counts the portion that comes from residual renewables on the grid.

In addition, in some areas Google is aiming to decarbonize the electricity sector by adopting a 24/7 carbon-free energy approach, matching data center electricity consumption with regional carbon-free energy.

Source: Georgiev 2019.

Box 3.3

DENMARK'S PURSUIT OF ENVIRONMENTALLY SUSTAINABLE DATA CENTERS

As part of its effort to reduce total greenhouse gas emissions by 70 percent by 2030, Denmark has established "climate partnerships" with 13 private sectors, including finance, food production and agriculture, life science and biotech, aviation, IT, and consulting. Each sector is to provide the government with concrete solutions on how to reduce greenhouse gas emissions in its field and to specify how policymakers can help them do so. In late 2020, Microsoft announced that it would make its most significant investment in Denmark yet, by constructing a hyperscale data center powered by 100 percent renewable energy.

Sources: https://op.europa.eu/en/publication-detail/-/publication/5ab1ada3-c48c-11e9-9d01-01aa75ed71a1/language-en; https://news.microsoft.com/europe/features/microsoft-announces-plans-to-establish-a-new-data-center-region-in-denmark-to-accelerate-the-countrys-green-digital-transformation/.

Several international standards and certifications on sustainable data centers are already in place. Metrics such as the aforementioned PUE, energy reuse factor (ERF), carbon usage effectiveness, and water usage effectiveness are all part of the standards on sustainability, IT, and data centers of the International Organization for Standardization.[22] Other large organizations have also established certifications and standards, including the Uptime Institute (Mytton 2021; Uptime Institute 2013) regarding renewable energy for data centers and the International Telecommunication Union (ITU) regarding procurement criteria for sustainable data centers.[23] In addition, in 2020, the European Commission published a working document on public procurement for data centers, server rooms, and cloud services to facilitate a more sustainable procurement process for public authorities. It also released the EU Code of Conduct for Energy Efficiency in Data Centers (European Commission 2020a, 2020b; Acton, Bertold, and Booth 2021). Box 3.3 provides details of Denmark's approach with pursuing environmentally sustainable data centers.

Regardless of which standard or certification is applied, adopting or migrating to public cloud services alters the IT risk landscape. Governments should consider five types of risk—data security and regulatory, technology, operational, vendor, and financial—before the process of migrating to the cloud begins, as outlined in Table 3.1 (Gadia 2018). A risk assessment can help identify a "first-mover"— a ministry or agency that is willing to take the lead in moving to the cloud. It can also identify the subsector or function within a ministry or agency that is best suited for migration to the cloud.

[22] https://www.iso.org/committee/654019.html.

[23] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14565.

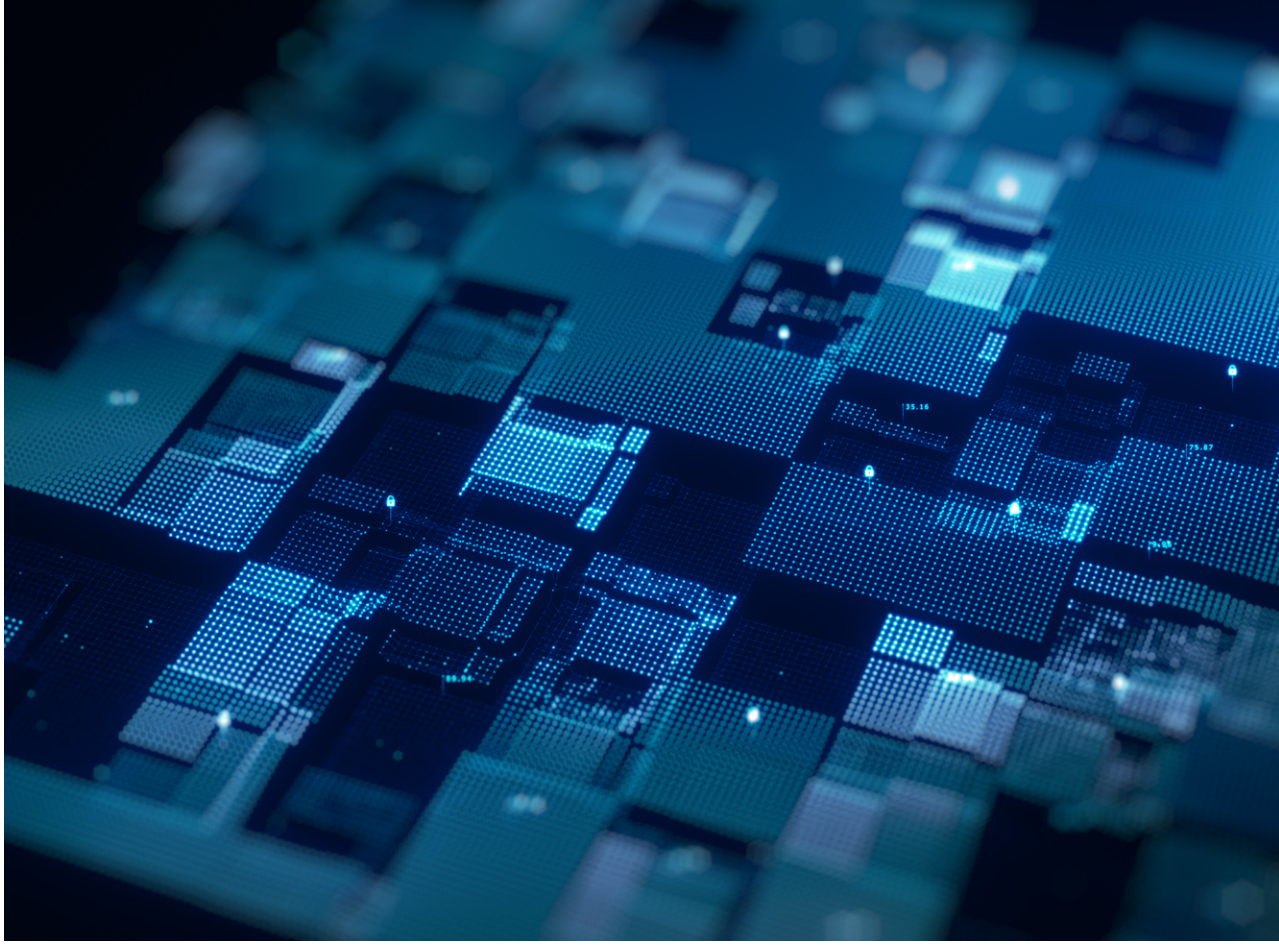


TABLE 3.1 Public Cloud Risks and Measures Governments can take to mitigate them

RISK CATEGORY	MEASURES FOR GOVERNMENTS TO MITIGATE RISK
Data security and regulatory	• Develop a governmental cloud strategy. • Develop a roadmap for cloud migration.
Technology	• Revise policies to update data governance to mitigate key risk categories.
Operational	• Involve security and risk professionals in cloud governance to mitigate vendor, data, technology, and operational risks.
Vendor	• Simplify cloud management processes to allow monitoring related to vendor, data, technology, and operational risks. • Ensure data protection requirements and hosting in accordance with data security legislation so as to mitigate vendor and data risks.
Financial	• Use advanced automation tools to benefit from the cloud and mitigate risks in all categories.

4. PATHWAYS FOR CLOUD MIGRATION

Once a government has decided to embark upon migration of data from legacy IT to some form of cloud services, there are various pathways and options, which are outlined in this section. Various considerations drive whole governments and individual agencies to consider migrating to the cloud. The government-as-a-whole approach focuses on larger, more fundamental IT investments with a long time span for return on investment, such as building high-throughput bandwidth connections or setting up a common master data scheme across government agencies. Government agencies on the other hand focus on how to solve a specific challenge such as managing COVID-19.

A government that takes no steps toward cloud solutions will maintain or develop legacy systems (storing data on-prem), often using software solutions or computer systems that are outdated and therefore difficult to manage, often either over-or-under-provisioned. This renders legacy systems as obstacles towards reaching advanced stages of digital development, including robust and sophisticated e-government platforms and services. Organizations may decide to retain a legacy system despite its long-term costs for several reasons, including the costs of upgrading to another system, a lack of trained personnel to manage the transition, and general misconceptions or uncertainties about new technologies.[24] But continuing to operate a legacy system carries high costs, such as increasingly expensive maintenance and replacement costs, problems with integration with software, and suboptimal cybersecurity in the face of a rapidly advancing thread landscape.[25]

Upgrading to cloud solutions has therefore become an increasingly attractive option, especially in terms of scalability, digital innovation, and data security.[26] Moreover, migration allows governments to take better advantage of Internet of

[24] https://www.talend.com/resources/what-is-legacy-system/.

[25] https://www.impactmybiz.com/blog/blog-legacy-systems-digital-transformation-risks-challenges/.

[26] https://www.impactmybiz.com/blog/blog-legacy-systems-digital-transformation-risks-challenges/.

Things (IoT) devices and technology,[27] develop web-scale IT,[28] and distribute workloads between the public cloud and on-prem data centers. The prospect of sharing workloads between a public cloud and on-prem equipment offers governments a new operating model that supports their IT departments' ability to combine and manage on-prem infrastructure or an internal private cloud with external cloud-based environments—community, public, or hybrid. In government, where consolidation is high on many agendas, a hybrid model requires very different competencies to support various public cloud deployments.

Governments that choose to migrate to cloud services have four basic options from which to choose, as outlined below.

Option 1: Migrate to the private cloud (with data stored on-prem). Private clouds are often used by government agencies, financial institutions, and other mid- to large-size organizations with business-critical operations that seek enhanced control over their environment.[29] For some organizations, the private cloud may be the only realistic option to ensure regulatory compliance. Many private cloud customers host data in their own data center or with a third-party cloud service. In either case, the services and infrastructure are kept on a private network, and the hardware and software are available to that customer alone. A private cloud can maximize legacy investment by retaining everything in-house—but at the cost of leaving a capital-intensive and high-cost structure in place.

Option 2: Migrate to a co-location data center (with data stored externally). Option 2 enables faster implementation, because it can obviate the need to build a new data center while providing some of the benefits of the public cloud, such as reducing the need for in-house technical staff. Essentially, it is an option to co-locate data server equipment by renting a co-location data center, also known as a third-party data center. At the same time, this option retains certain disadvantages such as high costs and limited ability to respond to demand surges.

---

[27] The IoT is the network of physical objects that contains embedded technology for communicating, monitoring, sensing, and interacting with multiple environments. For government, the IoT enables the digital transformation of service strategies. Government agencies can expect IoT-driven changes in several areas, including environmental and public infrastructure monitoring, emergency response, asset management, and traffic safety. Governments will need to approach the IoT strategically, evaluating how a growing base of intelligent objects and equipment can be combined with traditional IT systems to support innovations in operational performance and public service delivery.

[28] Web-scale IT is a system-oriented architectural pattern of world-class computing that delivers the capabilities of large cloud service providers within an enterprise IT organization. Organizations adopting a web-scale IT strategy will largely avoid the need to acquire expensive and scalable computing, storage, and networking resources; instead, they will be able to use low-cost, open-source hardware.

[29] https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/.

Option 3: Migrate towards a hybrid cloud (with data stored on-prem or in a private cloud alongside data stored or processed by public cloud service providers).

Option 3 combines the public and private cloud solutions, allowing data and applications to flow between the two locations (which may or may not require interoperability features). As noted earlier, hybrid cloud refers to the interconnectedness of on-prem or private cloud storage with public cloud. Many organizations and governments choose a hybrid option to enable them to address specific challenges, such as regulatory compliance, low Internet speed and quality, or greater security, while providing greater flexibility.[30] The hybrid solution offers some of the advantages of the public cloud, primarily cost-effective elastic surge capacity. "Hybrid-as-an-end-state" is used when some parts of the public workload can never be shifted to the public cloud. Under a "hybrid-as-net-new" approach, new projects move onto the public cloud. With this approach, all workloads will eventually be on the cloud as legacy systems are replaced, but the process occurs over a long period. Technology trends will change the landscape of these solutions, as edge computing makes public cloud solutions available in low-connectivity scenarios – a common setting in many developing countries. Some areas, such as defense, will always have strict limitations on use of the public cloud. It is also possible to use a hybrid cloud solution to interconnect workloads, without having data moved externally to the public cloud.

Option 4: Migrate to a public cloud (with data stored externally).

Option 4, the most widespread cloud computing option, is typically provided by a third-party company, which may or may not be a hyperscale cloud provider – though this is increasingly the case in markets and jurisdictions that provide an enabling environment for hyperscale public cloud solutions for many reasons discussed earlier in this guide. Though it's worth noting that some governments (e.g., Singapore) have set up their own public cloud, demonstrating alternative approaches governments have taken. In this model, the cloud service provider assumes all responsibility for the data centers, hardware, and infrastructure on which customer workloads run. The public cloud is delivered and accessible via the Internet and often provides web-based email, online office applications, storage, and other services.[31] To benefit fully from the low cost structure and rapid capacity increases offered by the public cloud, migration must be preceded by an appraisal of the legacy environment. In migrating to the public cloud, governments can use two or more cloud services from two or more cloud service providers. Customers may choose this option to avoid vendor lock-in, have more services to choose from, or ensure access to the latest innovations.[32] The approach has a higher barrier of entry, because greater technical skills are required to manage

---

[30] https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/.

[31] https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/.

[32] https://www.citrix.com/solutions/app-delivery-and-security/what-is-multi-cloud.html#:~:text=Multi%2D-cloud%20is%20a%20strategy,platforms%20to%20perform%20various%20tasks.&text=A%20multi%2D-cloud%20solution%20may,a%20service%20(IaaS)%20models.

different cloud infrastructures and the rigor of possible security measures can be no greater than those of the least-secure component of the hybrid arrangement. Table 4.1 summarizes the advantages and disadvantages of these four options, alongside legacy IT data storage.

TABLE 4.1 Advantages and disadvantages of legacy IT systems and 4 different cloud options

OPTION	ADVANTAGES	DISADVANTAGES
Maintain legacy IT systems (data stored on-prem)	• Business-as-usual resources are not shared with others; the configuration is maintained by an internal IT team.	• Capital costs for initial investment and training employees, operations, and maintenance can be high. • Facilities are often outdated and underutilized. • Legacy is inherently unable to scale beyond early defined requirements without capital investments. • The continuous existence of legacy systems will incur ever-increasing costs incurred for necessary integrations, mitigations, and so forth. • Inflexibility to meet fluctuating demand. • Unreliability because of lack of extensive backup systems needed to provide for disaster recovery capabilities. • Limited security capabilities
Migrate to private cloud (data stored on-prem)	• Hardware, data storage, and connection can be customized precisely to the desired task to assure some security with massive investments. • Regulatory compliance may be difficult for data classified as “top secret.”	• Flexibility to meet fluctuating demand is limited. • The lack of extensive backup systems to provide for disaster recovery may lead to unreliability. • Security capabilities are limited; private cloud solutions will struggle to stay on par with cloud-based security features.
Migrate to a co-location data center (data stored externally)	• External private clouds often offer more scalability than on-prem infrastructure. • Costs for training employees, operations, and maintenance are lower	• Visibility and control may be reduced, because of lack of tools to monitor deployments effectively.

Apply a hybrid cloud (interconnecting data stored on-prem or on private clouds with public clouds)	• Organization can maintain private infrastructure for sensitive assets or workloads that require low latency. • Additional resources on the public cloud can be accessed when needed. • Transitioning to the cloud need not be overwhelming, because migration can take place gradually, with workloads phased in over time.	• Interoperability can be challenge, as it is difficult to manage multiple disparate systems at the same time. • Additional infrastructure increases complexity. • Costs must be incurred for training employees, operations, and maintenance.
Migrate to public cloud (including hyperscale service providers)	• Capital costs are zero, as there is no need to purchase hardware or software. • New solutions can be tested almost immediately. • Service provider provides all maintenance. • Scalability is virtually limitless; on-demand resources are available to meet changing needs. • Reliability is high, as a vast network of servers ensures against failure. • Advanced features, such as artificial intelligence–enabled security, are provided.	• User loses control and visibility with regard to how and where data are stored and managed. • Data protection compliance requirements of every industry must be ensured. In countries with high regulatory complexity, data residency requirements may mandate that certain types of data be kept on-prem while other workloads can reside on the public cloud. • Shared security means that threats to security are also shared. • User may be locked into a vendor. This problem can be mitigated through a multicloud solution. However, a multicloud solution will increase interoperability challenges.

Source:
https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/#private-cloud.,

The choice between a public, private, or hybrid cloud depends on a variety of factors—and in the real world it is rarely an either/or situation. Countries have chosen different options. Singapore opted for a public cloud, launching its Commercial Cloud First Policy in 2018.[33] The main goal was to migrate the government's ICT systems onto the public cloud and to have at least 70 percent of less-sensitive government systems (such as human resources) hosted by the public cloud by 2023 (Government of Singapore 2018). Key reasons for transitioning to the public cloud included the greater availability and improved quality of public services, lower hosting costs, and reduced system downtime (Government of Singapore 2018).[34, 35]

[33] https://www.tech.gov.sg/media/technews/soaring-high-with-commercial-cloud.

[34] https://www.csc.gov.sg/articles/digital-government-smart-nation-pursuing-singapore%27s-tech-imperative.

[35] https://www.tech.gov.sg/media/technews/doubling-down-on-cloud-to-deliver-better-government-services.

Denmark chose the hybrid option. Denmark's Agency for Governmental IT Services provides IT services to 16 ministries and more than 28,000 users[36]. Its large on-prem data centers are expected to stay in operation for the foreseeable future, but the agency acknowledges the benefits of public cloud solutions, which it expects to use increasingly.[37] The country adopted a hybrid approach after assessing costs and benefits, including those related to data protection and the potential risk of vendor lock-in.[38]

The United Kingdom embraced the private cloud option. The UK Ministry of Defense (MoD) signed a 23-month deal with Microsoft Azure in May 2020, arguing that Azure's private cloud was the only one able to meet the ministry's technical and data protection needs.[39] In explaining its decision, the ministry also highlighted the need for direct access to cloud specialists and developers.[40]

Situations exist in which one option may be more suitable than another. For example, the public cloud is most suitable when cost efficiency (no upfront capital costs) is sought; demand peaks are unpredictable; and advanced features, such as AI–enabled security and other cutting-edge analytical tools and applications are needed. The private cloud may be more suitable for countries with rigid regulatory requirements, top-secret data classification, and organizations that can afford to continuously invest in high performance technology and well-trained IT personnel. The hybrid cloud may be best suited to organizations facing diverse security, regulatory, and performance requirements. The final section of this guide provides a framework for governments to use in navigating options for migrating to cloud services.

---

[36] https://www.computerworld.dk/art/254173/her-er-michael-oernoes-cloud-planer-for-statens-it-du-ser-ikke-os-drage-over-hals-og-hoved-ind-i-noget-cloud.

[37] https://www.computerworld.dk/art/254173/her-er-michael-oernoes-cloud-planer-for-statens-it-du-ser-ikke-os-drage-over-hals-og-hoved-ind-i-noget-cloud.

[38] https://www.computerworld.dk/art/254173/her-er-michael-oernoes-cloud-planer-for-statens-it-du-ser-ikke-os-drage-over-hals-og-hoved-ind-i-noget-cloud.

[39] https://www.computerweekly.com/news/252483650/MoD-cuts-through-competition-barriers-to-sign-direct-private-cloud-deal-with-Microsoft.

[40] https://ted.europa.eu/udl?uri=TED:NOTICE:236232-2020:TEXT:EN:HTML&src=0.

5. A DECISION FRAMEWORK FOR GOVERNMENTS NAVIGATING CLOUD MIGRATION OPTIONS

The decision-making model described in this section involves considerations at the policy, strategy, and operational levels. This three-layer model is structured around the government entity agency and highlights how much flexibility they have when considering cloud migration and shows how they can best utilize limited resources to generate the greatest benefit for the populace.

At the *policy level,* the goals of the migration—e.g., to improve services for citizens using the public cloud—are articulated. Decision making at this level includes an appraisal of the factors and trends affecting the migration decision and an assessment of the pace of innovation in the cloud services sector.

The *strategy level* considers the local context and identifies the areas most readily adaptable to public cloud solutions. It covers some of the constraints that governments face in the form of regulation, risk tolerance, and major societal investments that may affect the choice of projects that can be moved to the cloud.

The *operational level* focuses on the practical details of getting public cloud projects off the ground. It highlights what needs to be considered before commencing a project. Figure 5.1 illustrates the three-step framework for decision-making.

FIGURE 5.1 Three step framework for navigating cloud migration options

Policy-level decision making

Decision making at the policy level determines the objectives to be achieved and timing in connection with whether to adopt cloud solutions. Decisions are shaped by broad trends and developments in IT. The use of digital solutions has gradually seeped into the lives of most of the world's people. In particular, the rise of affordable mobile devices with Internet connectivity has opened the digital world to hundreds of millions of people across the globe.[41, 42] Governments face new expectations—from citizens and companies alike—to deliver digital solutions. This phenomenon has emphatically manifested in developed countries, and is increasingly taking shape in less developed countries.

For governments, the ability to access IT resources as needed offers multiple advantages. In emerging markets, the low cost and high flexibility of cloud solutions make a compelling value proposition, driving a growing demand for cloud services in e-education, e-health, e-commerce, e-business, e-governance, e-environment, and telecommuting (Kshetri 2010).

Within the public sector, implementation of cloud services facilitates access to resources and the analysis of large data sets. New technologies, mobile platforms, analytical tools, and enhanced e-citizen services will drive demand for data storage and digital infrastructure, both domestically and internationally. For example, government agencies can leverage cloud services to provide better health care, social amenities, justice, and public safety. Almost half of government organizations worldwide are already using cloud services.[43]

The cloud is also key to reducing energy use, as hyperscale computing is more efficient than individual servers and the proliferation of data centers. Public sector adoption of cloud services can thus advance clean energy policy goals.

Among the specific factors driving governments to the cloud are:[44]

- increasing collaboration among agencies and departments to improve web content using cloud applications
- promoting government efficiency through cloud-based applications and on-demand services
- allowing database access from different levels of government agencies that are attempting to solve particular public or policy problems
- providing online services to local governments, which otherwise would not have the infrastructure and technical capabilities to develop or contract these services

---

41 https://data.worldbank.org/indicator/IT.CEL.SETS?end=2019&most_recent_year_desc=-false&start=1960&view=chart&year=2016.

42 https://data.worldbank.org/indicator/IT.NET.BBND?end=2019&most_recent_year_desc=-false&start=1960&view=chart&year=2016.

43 https://www.gartner.com/smarterwithgartner/understanding-cloud-adoption-in-government/.

44 https://www.analyticsinsight.net/how-is-cloud-computing-helping-emerging-economies/.

- reaching citizens by providing a platform for them to propose actions and comment about government programs and services (digital citizen engagement applications)
- improving services to citizens through cloud portals that provide effective information.

There is a "mature state" for each country and government entity at which it stands to gain the greatest possible benefits from the cloud. The mature state can be understood as delivering public sector solutions using the public cloud to the degree that the entity's cloud readiness allows. Low cloud readiness may be characterized by low connectivity, highly restrictive regulation, weak digital capabilities, or all at once. Under such circumstances, the use of digital solutions powered by the public cloud will be low, and more local, private solutions will be more viable. Another important constraint to maturity is limited public cloud infrastructure. For example, hyperscale cloud providers play only a limited role in Africa, which makes latency-critical solutions difficult to implement (although there are notable exceptions, as described in Box 5.1). Other constraints include cultural barriers (inadequate natural language processing is still a hindrance for some less widely spoken languages), highly restrictive regulatory frameworks, and a lack of broadband and energy infrastructure.

Box 5.1

SOUTH AFRICA:
A case for the use of public cloud as the first African country with the presence of hyperscale providers

South Africa is home to most of the digital infrastructure in Sub-Saharan Africa. As such, the public sector, both government as a whole and individual public agencies, have access to a wide range of public cloud tools with high connectivity. South Africa represents the largest IT infrastructure capacity, including hyperscale regions, but also with several significant data centers construction planned. This capacity, however, is still not fully utilized in the public sector, though there are a few early adopters such as South Africa's National Department of Health and Apex Innovation. The COVID-19 pandemic has accelerated wider adoption of the public cloud across both business and government, and it is expected that South Africa will start migration of more workloads into the cloud. Interviews conducted for this guide found that the pandemic overloaded existing government IT infrastructure in many countries and so governments – like South Africa – began to shift workloads to the public cloud to manage scalability of government services. As the use of public cloud proliferates to more parts of the public sector, South Africa as a country will move into a higher mature state (Balancing Act 2021).

Source: Balancing Act 2021.

Evolving global trends in technological innovation will continue to redefine readiness, for example, by reducing the cost of Internet connectivity. 5G broadband mobile technology will increasingly permit the use of public cloud solutions. Edge computing is making it easier to construct solutions centrally while deploying them locally (Khan et al. 2019).[45] Other advanced technologies, such as AI and quantum computing, are expected to significantly increase the adoption of cloud computing services.[46]

A list of key questions at the policy level that can help government officials assess the "mature state" include the following:

- Where are the data to be stored?
- Who will manage the data?
- Is additional training needed?
- Would the benefits after the migration exceed the costs? If so, by how much?
- What are the indirect benefits, costs, and risks of each option?
- Will the cloud or data storage system be interoperable with other government agencies that may benefit from accessing the data?
- Are there any data localization or data protection requirements that may hamper the use the of cloud?
- Are there any guidelines to assist governments in procuring cloud solutions?
- Which public sectors are a priority?
- Which government services are to be prioritized (for example, vehicle registration, change of residency, registering a company)?
- What are the basic components of the IT architecture needed (for example, digital ID, secure mailbox, digital payment)?
- Can the approach be easily scaled up?
- Are there country-specific legal issues?

A broad government policy for enabling digital transformation can be a powerful catalyst to increase cloud readiness. It can help demystify use of cloud services – and in particular the public cloud where there is greater misunderstanding and inquiry – and show how it can be used to solve concrete public issues. Cloud readiness can be increased by introducing robust risk-management frameworks, such as Japan's Ismap or the United States' FedRAMP, which help government agencies adopt and use modern cloud technologies in a secure and uniform manner.[47] To increase cloud readiness, the policy should address the barriers blocking public sector entities from adopting the public cloud. Some of the issues the policy should cover includes the following:

---

[45] https://www.technologyreview.com/2021/05/24/1025131/edge-computing-powering-the-future-of-manufacturing/.

[46] https://www.mckinsey.com/industries/public-and-social-sector/our-insights/when-governments-turn-to-ai-algorithms-trade-offs-and-trust.

[47] https://www.gsa.gov/technology/government-it-initiatives/fedramp.

- a data classification scheme, as seen in the UK Cloud First strategy
- a regulatory framework in which public cloud solutions are not dismissed out of hand even if no legal barriers exist
- knowledge about approaches in low-connectivity situations (for example, how localized cloud deployments or edge computing can help solve cloud adoption challenges)
- budgetary guidance on incorporating public cloud scaling cost structures into governmental budget processes (moving from capital expenditures to operating expenditures).

The United Kingdom's application of its Cloud First policy offers an example of how these issues can be handled. This Cloud First policy encourages all public sector organizations to consider and evaluate cloud solutions before other options.[48] A primary objective is to modernize public services.[49] The strategy is mandatory for the central government and strongly recommended for the broader public sector.[50] The United Kingdom continues to follow the General Data Protection Regulation (GDPR) framework on data localization.[51] But recognizing that different ministries deal with different challenges and that a one-size-fits-all cloud solution does not exist, the government allows ministries and departments to choose an alternative to cloud solutions. However, any such alternative must offer better security, flexibility, and value for money spent, defined as "the best mix of quality and effectiveness for the least outlay over the period of the use of the goods or services bought" (HM Treasury 2021).[52, 53] Appendix B provides other examples of country initiatives supporting governmental adoption of cloud solutions.

Regulation is a critical factor that affects how cloud services can be used by a government in two major ways. First, it sets rules for how public sector entities should behave. Second, regardless of its intent, it may lead to unintended consequences. Fear of unknown consequences could lead public sector entities to refrain from using public cloud services even if the cloud might be the most beneficial tool for the challenge at hand (ACCA 2019). While it is beyond the scope of this report to provide or recommend specific policies for use by public sector regulators, governments that want to facilitate public cloud solutions would generally need to refrain from drafting policies that limit the scope for unintended consequences by setting clear rules and keeping in mind the tradeoffs of restrictive data localization requirements and certification processes. Unintended effects are often correlated with overly stringent certification processes, broadly restrictive data classification

---

48 https://www.gov.uk/guidance/government-cloud-first-policy.

49 https://technology.blog.gov.uk/2019/10/31/cloud-first-is-here-to-stay/.

50 https://www.gov.uk/guidance/government-cloud-first-policy.

51 The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third-party countries, and to international organizations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined. It does not introduce or include any data residency or localization obligations. The GDPR's predecessor, the Data Protection Directive (95/46/EC), also included no data residency or localization obligations. The GDPR does ban storage of data outside the European Union, although personal data about air passengers are shared more liberally.

52 https://technology.blog.gov.uk/2019/10/31/cloud-first-is-here-to-stay/.

53 https://www.gov.uk/guidance/government-cloud-first-policy.

schemes, and cumbersome procurement processes (Levite and Kalwani 2020; AWS 2019). The aforementioned Cloud First policy of the UK is a prime example of how a government can tailor a policy to enable optimal cloud maturity.

The reason data localization is at the forefront of cloud policy discussions is that these requirements legally define how specific types of data are to be processed and stored within a country or a union of countries. Before migrating to the cloud, governments and ministries would benefit from identifying which data are intended to be located on the cloud, as laws often distinguish between types of data. For instance, publicly available data in official registers are likely to have less strict localization requirements than personal data on health or finances.

To facilitate data classification, an example from Nigeria below is useful to demonstrate how a government has approached creating a data-classification framework to help ministries and other public entities determine what types of data can be located on public cloud solutions and potentially located outside the country (Table 5.1) (NITDA 2019). Nigerian ministries and agencies are focusing on moving less-sensitive data to the cloud first (NITDA 2019). This data classification framework helps ministries decide what cloud solution best fits its needs.

TABLE 5.1 Cloud solutions based on level of data sensitivity

LEVEL OF DATA SENSITIVITY	CLOUD SOLUTION
National security information	Custom, hardened, on-prem systems
Sensitive government business or citizen data	Private and/or hybrid cloud solutions with enhanced security controls
Routine government business	Public cloud solutions with industry standard security are suitable
Public or nonconfidential information	

Strategy-level decision making

Several choices need to be made at the strategy level when planning a public cloud migration. The first step is to identify a ministry or agency with relatively high cloud readiness to take the lead. Ministries of health or defense often deal with highly sensitive data such as personal health records and military assessments related to national security. The data held by ministries of tourism and transport are less complex and sensitive. Data on the numbers of tourists entering a country or public transport data can easily be migrated to the cloud, should the decision be made to do so.

Within a ministry, the first strategic step is determining what data are suitable for the cloud, and more narrowly, the public cloud (if any). At this level, data classifications should focus on the data type, data throughput, and integration options rather than data residency requirements. Keeping data on-prem does not necessarily improve security, given the state-of-the-art AI security features that are available on the public cloud but often not in-house due to high cost.

Structured data of low complexity and high throughput are highly suitable for cloud migration. For example, sensor data from trains make a good fit for the public cloud, while human resources data on employees may be more suitable for private cloud options.

For governments that want to migrate to public cloud servers, a clear system for data classification is essential in identifying which type of data can be moved to the public cloud. Several data classification regulations and standards exist, including the GDPR scheme, NIST 800-53, and ISO 27001. NIST 800-53 from the U.S. National Institute of Standards and Technology specifies that data must be categorized by level of security in order to pass a compliance audit (NIST 2017). ISO 27001 is an international standard for the establishment, implementation, maintenance, and improvement of an information security management system. To pass an ISO 27001 audit, organizations must show a good understanding of the value of their assets, prove ownership of the data, and explain how internal data are handled.[54]

Data complexity varies across ministries and agencies. Establishing a ministry or agency with relatively high cloud readiness to take the lead in migrating to the cloud is a key strategic step. As a practical example, ministries of health or defense often deal with data that can be classified as highly sensitive, as the data mix might include personal health records, military assessments related to national security, and so forth. It is different with less sensitive ministries, for example tourism and transport, as the complexity and sensitivity of the data are much lower. In this sense, it is highly relevant for governments and ministries to assess data complexity and sensitivity before deciding which agency or ministry should move to the cloud first.

The benefits of transitioning to the cloud depend on the willingness to invest in various digital solutions, although even at a small scale migrating to the cloud will bring valuable knowledge and provide in-house IT staff with the right skills.[55] Cautious governments and ministries might adopt a "lift-and-shift" strategy, which entails simply migrating an existing legacy system to the cloud, though such a strategy can be risky, however, because legacy systems may not be correctly designed for the cloud, which can limit the ability to scale up when needed.[56] To mitigate these risks, any commitment to a cloud transition should involve a restructuring of legacy systems so that they are aligned with the security and capacity requirements of the cloud.[57] Several factors in addition to legacy systems will affect the type of cloud solution that is appropriate for a particular government or ministry—chief among them data connectivity, data control, IT skills, and the budget process. Several of these topics are touched on briefly below.

---

[54] https://www.iso.org/isoiec-27001-information-security.html.

[55] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/cloud-adoption-to-accelerate-it-modernization.

[56] https://www.prescientsolutions.com/blog/how-deep-is-your-commitment-to-cloud/.

[57] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/cloud-adoption-to-accelerate-it-modernization.

Data connectivity is an important because cloud and hyperscale data centers rely on well-connected, fast broadband infrastructure. While broadband is widespread in more developed countries, it is less established in developing, lower-income countries. The greater the connectivity, the greater the potential benefits of using the cloud. But even in low-connectivity situations, the cloud can unlock potential benefits—via edge computing, for example. Edge computing refers to completing a computing task locally ("at the edge") on an IoT device, instead of sending it to a data center located elsewhere and waiting for a response. Use of this type of technology has seen a significant increase in the developed world because of its superior performance in high-throughput scenarios and its ability to strengthen infrastructure. Edge computing and IoT connectivity is now possible because of innovations in the way chipsets can be designed to function even in miniature devices, as well as better-developed software to orchestrate both the local handling and the deployment of these devices. Using IT devices requires power, but edge computing can rely on solar- or battery-powered devices when the power supply is unstable – conditions more common in developing countries. Most variants of IoT have even built-in "event handling," meaning the device can queue up messages and send them to a central service when power is restored, reducing the impact of outages.

As the hyperscale cloud services providers have expanded to cover more countries and different use cases, the demand for a localized version of some public cloud features has increased.[58] This development has been driven by advancements in edge computing. Several hyperscale cloud providers now offer some variant of edge public cloud technology, typically a physical device that allows government entities to use some of the benefits of the cloud even in circumstances of extremely poor connectivity. For example, it is possible to gain access to localized storage resources from which processed data can be transferred to the cloud when connectivity allows, using solutions such as AWS Outposts or GCP Anthos.[59] Governments in developing countries can thus navigate a path toward the mature state—reaping the benefits of public cloud tools—even if connectivity remains a challenge.

Laws governing the control of data vary. The European Union's GDPR provides one of the strictest data protection frameworks in the world, with fines for overstepping GDPR as high as €20 million, or 4 percent of global revenue (whichever is higher).[60] Singapore's Personal Data Protection Act (PDPA) shares some similarities with the GDPR, but it differs in some respects. For example, the PDPA excludes public agencies from its scope (OneTrust DataGuidance 2020). National governments should assess their legal frameworks and determine how they will affect the use of cloud solutions, and in particular, public cloud services.

---

[58] https://www.cio.com/article/3615274/where-cloud-and-edge-meet.html; https://www.infoworld.com/article/3616576/edge-computing-can-be-a-data-cache-for-public-clouds.html.

[59] https://aws.amazon.com/snowball/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc; https://azure.microsoft.com/en-us/services/databox/; https://cloud.google.com/anthos, https://aws.amazon.com/outposts/.

[60] https://gdpr.eu/what-is-gdpr/.

The IT skills needed to build technology infrastructure are by no means evenly distributed around the world. Levels of digital skills are generally high in developed countries, including more advanced and sophisticated digital literacy regarding emerging technologies; by contrast, digital skills – particularly at the more advanced level – are lower in developing countries. The more advanced digital skills related to cloud computing include programming, platform expertise (AWS, Google Cloud Platform, Microsoft Azure, and so forth), maintaining of databases, and data security. National government and ministries must ensure the presence of adequate staff before migrating to the cloud (even while recognizing that one of the key benefits of adopting public cloud solutions is off-loading much IT service responsibility to the vendor). And because rapid technological advancements make it difficult to remain up to date on all possible cloud opportunities, technical specialists should be available to inform officials about the latest developments.

As noted above, legacy systems are challenges to cloud migration. Often woefully outdated and expensive to maintain,[61] legacy systems stifle the adoption of new solutions, hampering performance.[62] Paradoxically, a complete absence of legacy systems may ease the move to the cloud, and governments in developing countries may have an opportunity to take advantage of this scenario, in the presence of a cloud-enabling environment. A good example of such "leapfrogging" mechanisms can be seen with Chinese companies that have foregone the cumbersome IT systems that bog down many western companies and moved directly into public cloud alternatives (Wu, Du, and Wei 2004; Chen and Li-Hua 2011).

As a government cloud migration inevitably requires public investments, nontransparent or incomplete budget processes make it difficult for public entities to plan a migration to the cloud and for private investors to decide whether to invest in a given country. National government budgeting is therefor a critical exercise as it allocates financial resources to different ministries, agencies, and other public entities to sustain and improve the quality of their respective society.[63] A successful budget process thus allows for governments to manage, prioritize, and plan for its financial resources, and can determine the trajectory of cloud migration.

Operational-level decision making

The operational considerations identified here are intended for both government-as-a-whole and individual ministries or agencies. A broad, all-encompassing governmental IT strategy need not be in place before a ministry can consider using the public cloud to solve concrete challenges, although adoption of a broad digital strategy eases barriers to entry and can empower ministries to embark on the digital journey by taking operational steps.

A significant operational step public sector entities in developing countries and elsewhere must deal with is the task of entering into an agreement with a cloud

[61] https://www.prescientsolutions.com/blog/how-deep-is-your-commitment-to-cloud/.

[62] https://www.imaginovation.net/blog/legacy-systems-slow-down-business-growth/; https://www.capgemini.com/2020/12/how-legacy-systems-are-holding-businesses-back/.

[63] https://pdf4pro.com/view/the-budgeting-process-department-of-budget-2deaac.html.

service provider. Overall, the general process of purchasing cloud services is highly analogous to other government procurement processes. For cloud solutions, this involves (1) creating a request for proposal (RFP), and identifying the minimum requirements a vendor must meet; (2) assessing the winning proposals; (3) selecting a vendor, and (4) signing a service agreement. A manual developed by CISPE (Cloud Infrastructure Services Providers in Europe) can help guide the process (CISPE 2020; Center for Digital Government 2018).

For governments – as well as commercial entities – it is important and beneficial to avoid becoming locked into any single cloud vendor. Vendor lock-in is a situation in which a client becomes dependent on a provider because the service or solution has become so deeply integrated it is difficult to switch to a different one (Hong et al. 2019). The remedy for reducing the risk of vendor lock-in depends to a large extent on the type of service being used. In general, the more of a service that is managed by the cloud provider, the harder it is to avoid vendor lock-in. A SaaS arrangement is the most difficult to shift to a different vendor, while IaaS is easier to move, because the core features are the same across most hyperscale cloud providers.

Regardless of which type of cloud service is used, governments and government agencies can consider a multi-cloud strategy that makes it easier to switch between vendors and avoids being locked-in by vendors. This strategy should entail, among other things, the core data model and an architectural drawing of the mechanisms of the solution (Kratzke and Quint 2017; Hong et al. 2019; Sandobalin, Insfran, and Abrahao 2018).

It is prudent to use infrastructure as code (IaC) as the basis for any technical solution. IaC is a recipe for building IT solutions with public cloud services. It also makes it easier for users to shift from one cloud vendor to another in a significantly reduced timeframe. At the onset, IaC was tailored specifically for a given CSP, though within the last couple of years open-source coding tools have enabled for writing vendor agnostic "recipe files." This allows a public entity to make an application that is easily shiftable between different CSPs which fosters a robust multi-cloud approach for the public sector and thus reduces the risk of vendor lock-in.

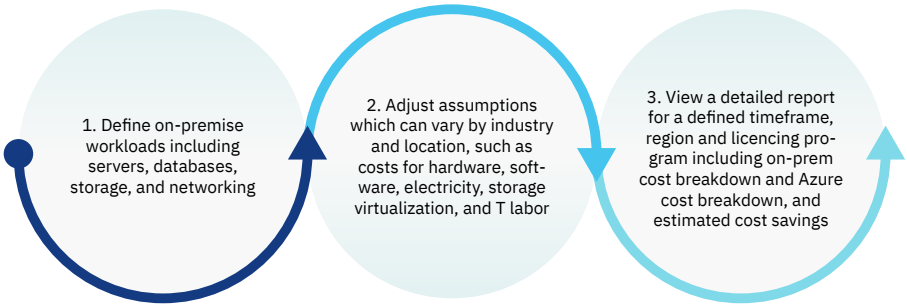
But the essential recommendation is to create a solution team with "DevOps" competencies (Ebert et al. 2016; Leite et al. 2019). The DevOps approach and culture emphasizes continuous development in response to feedback, discouraging the tendency to plan too far into the future and enabling the organization to adapt quickly to changes. Planning focuses on smaller deliverables for faster development and delivery.[64] As a central feature of the DevOps process, IaC decreases development time by enabling changes to the solution to be rolled out almost immediately—and rolled back in the event of errors or unforeseen problems.

[64] This effect has been seen in public sector initiatives in Singapore. See https://www.tech.gov.sg/media/technews/doubling-down-on-cloud-to-deliver-better-government-services.

Moving spending to the operating budget is also a critical operational consideration. Traditionally, public institutions have purchased IT through capital spending, receiving a certain allocation of capital over a fixed-term, multiyear contract. This mechanism clashes with the government's need to constantly update IT as the pace of innovation makes technology obsolete on a regular basis. As a result, governments are unable to harness benefits from newer, more flexible technologies that allow for smarter spend and better delivery through pay-per-use, on-demand cloud services (an operational expenditure). The fact that capital and operating expenses are budgeted separately makes it difficult for government entities to pay for cloud services. Ministries of finance and other treasury bodies could authorize the reallocation of planned capital spending for digital technology to the operating budget. In the absence of ongoing investment, technology decays, data integrity declines, and innovation slows. The legacy approach based on capital spending locks public institutions into investments and structures that soon leave them with outdated technology.

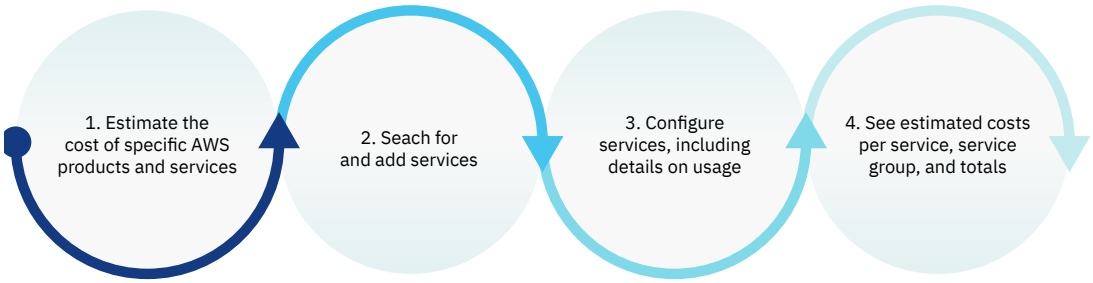
Cloud providers can help potential clients estimate the costs and potential savings of migrating workloads to the public cloud. Nearly all hyperscale cloud providers offer cost calculators that help perform these calculations, but it is important to make sure the analysis is not based solely on what a single vendor tool can identify or provide. It is also important to review the risks that could affect the cost-benefit calculations. Figures 5.2 and 5.3 illustrate the process used by the two well-known hyperscale cloud providers.

FIGURE 5.2 Process for calculating total cost of ownership with Microsoft Azure



Source: https://azure.microsoft.com/en-us/pricing/tco/calculator/.

FIGURE 5.3 Process for calculating total cost of ownership with the AWS pricing calculator



Source: https://calculator.aws/#/.

Once a migration decision is made and a provider is chosen, the parties must enter into an agreement, known as a service level agreement (SLA). An SLA specifies what services and guarantees the cloud provider will supply. The cloud provider offers financial backing for its commitment to achieve and maintain the levels for each service. If it does not achieve and maintain those levels, the cloud user may be eligible for a credit toward a portion of the monthly service fees.[65] Cloud providers typically promise high availability and reliability, which are usually documented in the SLA. Governments should ensure SLAs include assurances on service availability, data ownership, hardware and software specification, disaster recovery plans, and customer responsibilities. Addressing these in the SLA helps prevent unintended negative consequences. For example, agreeing that data will be stored for at least five years before being deleted or returned as a physical copy would help allay fears that data might be permanently lost. Appendix E provides an illustration of a 'mind-map' structure of a cloud-specific SLA.

Once technical development commences, an agile development process helps ensure that the technical product addresses the core "pain point" (Papatheocharous and Andreou 2014). It is crucial to avoid trying to address all possible infrastructure problems before the start of the project but rather to allow engineers the opportunity to solve problems in iterations, using the solutions available to them. Part of this process is investigating whether a SaaS solution is available, rather than building a custom solution for every problem (Benlian, Koufaris, and Hess 2010).

The policy, strategy, and operational factors described in this section focus on actionable recommendations that can be used by public entities to take their first steps toward using cloud services to solve challenges and improve service delivery. Table 5.2 provides a summary of key questions decision-makers at each level should consider as discussed in this section. Readers can refer to Appendix B-D for examples of policy, strategy, and operational initiatives supporting government cloud adoption, and are encouraged to refer to the sources provided for more granular context of the examples from both developed and developing country contexts.

[65] https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=18897.

TABLE 5.2 Policy, strategy, and operational decisions made at whole-of-government and ministry or agency levels

	LEVEL OF GOVERNMENT	
Type of decision	Whole of government	Ministry or agency
Policy: What direction do we take, and how quickly do we move?	• Types of decision and options a national agency could make	• Types of decision and options a ministry or agency needs to make
Strategy: What are our objectives?	• What central functions should be engaged? • What "cloud-readiness factors" can be improved (for example, data localization laws)? • Which agency should take the lead?	• What subsectors or functions are most suited? • Should transition legacy systems or only new projects be moved to the cloud? • What level of investment should be made?
Operational: How do we begin?	• What policy steps are useful to focus on for enabling optimal cloud migration across government units? • How can ministries be enabled to account for data classification in a process to identify priorities?	• Within the identified priority areas, what is the most cost-effective system to transition to? • How can the right solution be procured? • How can vendor lock-in be avoided?

The three-step framework has been identified and described partly on the available literature highlighting problematic matters but also based on issues faced by World Bank task teams and interviews with clients in developing countries. While the COVID-19 pandemic triggered a rapid acceleration of public sector entities adopting cloud solutions to help solve scaling and deployment speed issues, cloud-based solutions were already being adopted quickly across the globe, and this growth is expected to continue beyond the pandemic. As citizen needs and demands continue to grow, especially in developing countries, governments who harness cloud-based solutions will be better positioned to meet these growing demands in the most effective way possible, with a variety of public and private cloud options and hybrid and multi-cloud architectures available to facilitate IaaS, SaaS, and PaaS solutions.

REFERENCES

ACCA (Asia Cloud Computing Association). 2019. *From Vision to Procurement: Principles for Adopting Cloud Computing in the Public Sector.* https://asiacloudcomputing.org/research/.

Acton, Mark, Paolo Bertold, and John Booth. 2021. "2021 Best Practice Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency." JRC Technical Notes no. JRC123653, Joint Research Centre, European Commission, Ispra, Italy. https://e3p.jrc.ec.europa.eu/publications/2021-best-practice-guidelines-eu-code-conduct-data-centre-energy-efficiency.

Al-rimy, Bander Ali Saleh, Mohd Aizaini Maarof, and Syed Zainudeen Mohd Shaid. 2018. "Ransomware Threat Success Factors, Taxonomy, and Countermeasures: A Survey and Research Directions." *Computers & Security* 74 (May): 144–66.

AWS (Amazon Web Services). 2019. *Cloud First Playbook for Asia Pacific (APAC).* https://d1.awsstatic.com/Digital%20Marketing/Institute/Cloud_First_Playbook_APAC.pdf.

Balancing Act. 2021. *Africa Interconnection Report: Analysis of Sub-Saharan Africa's Cloud & Data Centre Ecosystem.* https://info.consoleconnect.com/resources/console-connect-africa-interconnection-report-lp?hsLang=en.

Benlian, A., M. Koufaris, and T. Hess. 2010. "The Role of SaaS Service Quality for Continued SaaS Use: Empirical Insights from SaaS Using Firms." Proceedings of the 31st International Conference on Information Systems (ICIS 2010), St. Louis, Florida, December 12–15. https://www.en.dmm.bwl.uni-muenchen.de/pubdb_en/art_proc_i/2010-02.html.

Center for Digital Government. 2018. "Understanding Cloud Procurement: A Guide for Government Leaders." https://www.oracle.com/us/industries/public-sector/understand-cloud-procurement-wp-4423120.pdf.

Chen, Dezhi, and Richard Li-Hua. 2011. "Modes of Technological Leapfrogging: Five Case Studies from China." *Journal of Engineering and Technology Management* 28 (1–2): 93–108. ISSN 0923-4748.

CISPE (Cloud Infrastructure Services Providers in Europe). 2020. *Buying Cloud Services in Public Sector*. https://cispe.cloud/website_cispe/wp-content/uploads/2020/06/CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v-EN-2020-05-11.pdf.

Danish Government. 2018. *Strategy for Denmark's Digital Growth.* Ministry of Industry, Business, and Financial Affairs, Copenhagen. https://eng.em.dk/media/10566/digital-growth-strategy-report_uk_web-2.pdf

Danish Ministry of Finance. 2016. *A Stronger and More Secure Digital Denmark: Digital Strategy 2016–2020.* Danish Ministry of Finance, Local Government Denmark, and Danish Regions. https://en.digst.dk/media/14143/ds_singlepage_uk_web.pdf

Daub, Matthias, and Niels Gotfredsen. 2019. "Defining a public cloud strategy: An interview with Michael Orno of Denmark's Statens IT," McKinsey & Company, June 29. https://www.mckinsey.com/industries/public-and-social-sector/our-insights/defining-a-public-cloud-strategy-an-interview-with-michael-orno-of-denmarks-statens-it

Daub, Matthias, Axel Domeyer, Abdulkader Lamaa, and Frauke Renz. 2020. "Digital Public Services: How to Achieve Fast Transformation at Scale." McKinsey & Company. https://www.mckinsey.com/~/media/McKinsey/Industries/Public%20and%20Social%20Sector/Our%20Insights/Digital%20public%20services%20How%20to%20achieve%20fast%20transformation%20at%20scale/Digital-public-services-How-to-achieve-fast-transformation-at-scale-vF.pdf.

Deloitte. N.d. "Data Privacy in the Cloud: Navigating the New Privacy Regime in a Cloud Environment." Deloitte, Canada. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-privacy-in-the-cloud-pov.PDF.

Ebert, C., G. Gallardo, J. Hernantes, and N. Serrano. 2016. "DevOps." *IEEE Software 33* (3): 94–100.

European Commission. 2020a. "EU GPP Criteria for Cleaning Services." Commission Staff Working Document, European Commission, Brussels. https://ec.europa.eu/environment/gpp/pdf/20032020_EU_GPP_criteria_for_data_centres_server_rooms_and%20cloud_services_SWD_(2020)_55_final.pdf.

European Commission. 2020b. *Development of the EU Green Public Procurement (GPP) Criteria for Data Centres, Server Rooms and Cloud Services.* Luxembourg: Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/89971797-a9fa-11ea-bb7a-01aa75ed71a1/language-en.

European Environment Agency. 2020. *Country Maturity Report: Republic of Moldova.* June. https://eni-seis.eionet.europa.eu/east/areas-of-work/access-to-environmental-information/products/moldova-country-maturity-report

Gadia, Sai. 2018. "How to Manage Five Key Cloud Computing Risks." KPMG, Canada. https://assets.kpmg/content/dam/kpmg/ca/pdf/2018/03/cloud-computing-risks-canada.pdf.

Georgiev, Ivo. 2019. "Competitiveness of Corporate Sourcing of Renewable Energy: Annex A.3 to Part 2 of the Study on the Competitiveness of the Renewable Energy Sector: Case Study: Google." Publications Office of the European Union, Luxembourg. https://op.europa.eu/en/publication-detail/-/publication/5ab1a-da3-c48c-11e9-9d01-01aa75ed71a1/language-en.

Government of Singapore. 2018. "Digital Government Blueprint 'A Singapore Government that Is Digital to the Core, and Serves with Heart.'" Government of Singapore, Singapore. https://www.tech.gov.sg/files/media/corporate-publications/dgb-public-document_30dec20.pdf.

HM Treasury. 2021. *Managing Public Money.* United Kingdom: HM Treasury. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742188/Managing_Public_Money__MPM__2018.pdf.

Hong, J., T. Dreibholz, J. A. Schenkel, and J. A. Hu. 2019. "An Overview of Multicloud Computing." In *Web, Artificial Intelligence and Network Applications, WAINA 2019*. Advances in Intelligent Systems and Computing Series, vol. 927, edited by L. Barolli, M. Takizawa, F. Xhafa, and T. Enokido, 1055–68. Cham, Switzerland: Springer.

IEA (International Energy Agency). 2021. *Data Centres and Data Transmission Networks*. Paris: IEA. https://www.iea.org/reports/data-centres-and-data-transmission-networks.

Kaloudi, Nektaria, and Jingyue Li. 2020. "The AI–Based Cyber Threat Landscape: A Survey." *ACM Computing Surveys* 53 (1): 1–34.

Khan, Wazir Zada, Ejaz Ahmed, Saqib Hakak, Ibrar Yaqoob, and Arif Ahmed. 2019. "Edge Computing: A Survey." *Future Generation Computer Systems* 97 (August): 219–35.

KPMG. 2014. "Cloud Economics: Making the Business Case for Cloud." https://assets.kpmg/content/dam/kpmg/pdf/2015/11/cloud-economics.pdf.

Kratzke, N., and P. C. Quint. 2017. "Understanding Cloud-Native Applications after 10 Years of Cloud Computing: A Systematic Mapping Study." *Journal of Systems and Software* 126 (April): 1–16.

Kshetri, Nir. 2010. "Cloud Computing in Developing Economies." *IEEE Computer* 43 (10): 47–55. https://ssrn.com/abstract=2015387.

Leite, L., C. Rocha, F. Kon, D. Milojicic, and P. Meirelles. 2019. "A Survey of DevOps Concepts and Challenges." *ACM Computing Surveys 52 (6):* Article 127, pp. 1–35.

Levite, Ariel E., and Gaurav Kalwani. 2020. "Cloud Governance Challenges: A Survey of Policy and Regulatory Issues." Working paper, Carnegie Endowment for International Peace, Washington, DC. https://carnegieendowment.org/2020/11/09/cloud-governance-challenges-survey-of-policy-and-regulatory-issues-pub-83124.

Malwarebytes Lab. 2020. *2020 State of Malware Report.* https://www.malwarebytes.com/resources/files/2020/02/2020_state-of-malware-report.pdf.

Mytton, David. 2021. *Renewable Energy for Data Centers.* UI Intelligence report 44. Seattle, WA: Uptime Institute. https://uptimeinstitute.com/publications/asset/renewable-energy-for-data-centers.

NCSC (National Cyber Security Centre). 2020. "Security Benefits of a Good Cloud Service." Whitepaper, NCSC, November 13. https://www.ncsc.gov.uk/whitepaper/security-benefits-of-a-good-cloud-service.

NIST (National Institute of Standards and Technology). 2017. *Security and Privacy Controls for Information Systems and Organizations.* Draft NIST Special Publication 800-53, Revision 5. Gaithersburg, MD: NIST. https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf.

NITDA (National Information Technology Development Agency). 2019. *Nigeria Cloud Computing Policy*. Nigeria: NITDA. https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf.

OneTrust DataGuidance. 2020. *Comparing Privacy Laws: GDPR v. Singapore's PDPA.* https://www.dataguidance.com/resource/comparing-privacy-laws-gdpr-v-singapore-pdpa.

Papatheocharous, E., and A. S. Andreou. 2014. "Empirical Evidence and State of Practice of Software Agile Teams." *Journal of Software: Evolution and Process* 26 (9): 855–66.

Ponemon Institute. 2014. *The State of Data Centric Security*. Traverse City, MI: Ponemon Institute. https://www.informatica.com/content/dam/informatica-com/en/collateral/analyst-report/gated/en_state-of-data-centric-security-ponemon_analyst-report_2660.pdf?uid=12-27304.

Rawat, A., A. Singhal, and T. Choudhury. 2021. "Toward Securing Cloud & Information: Vision & Challenges." *11th International Conference on Cloud Computing, Data Science & Engineering (CONFLUENCE):* 220–26. doi: 10.1109/Confluence51648.2021.9377125.

Sandobalin, J., E. Insfran, and S. Abrahao. 2018. "An Infrastructure Modeling Approach for MultiCloud Provisioning." In *Information Systems Development: Designing Digitalization (ISD2018 Proceedings)*, edited by B. Andersson, B. Johansson, S. Carlsson, C. Barry, M. Lang, H. Linger, and C. Schneider. Lund, Sweden: Lund University.

SAP. 2020."SAP: Helping Australians Get Back to Work." SAP Public Policy Paper, SAP, Australia. https://www.sap.com/australia/documents/2020/05/b85cc684-9a7d-0010-87a3-c30de2ffd8ff.html.

Solomon, Shoshanna. 2021. "Amazon, Google reportedly oust Microsoft, Oracle in massive Israel cloud tender." *The Times of Israel,* March 31. https://www.timesofisrael.com/amazon-google-reportedly-oust-microsoft-oracle-in-massive-israel-cloud-tender/

Uptime Institute. 2013. "Tier Standard: Operational Sustainability." https://uptimeinstitute.com/publications/asset/tier-standard-operational-sustainability.

World Bank. 2021. "Knowledge Pack: Cloud for Education." World Bank, Washington, DC.

World Bank IEG. 2017. "Moldova e-Transformation." Implementation Completion Report Review, Independent Evaluation Group, World Bank, Washington, DC. https://documents1.worldbank.org/curated/en/672011507844559743/pdf/ICRR-Disclosable-P121231-10-12-2017-1507844546788.pdf

Wu, Emily. 2021. *Sovereignty and Data Localization*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/sovereignty-and-data-localization.

Wu, X. B., J. Du, and S. J. Wei. 2004. "Leapfrogging Ways of Manufacturing Industry in China Driving by IT." *2004 IEEE International Engineering Management Conference (IEEE Cat. No.04CH37574)* 2: 860–64. doi: 10.1109/IEMC.2004.1407504.

APPENDIX

Appendix A. A selection of cloud standards and accreditations that can help guide navigating options amongst cloud service providers

- Federal Risk and Authorization Management Program (FedRAMP)
- Service Organization Controls (SOC) 1/American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] No. 16)/International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70), SOC 2, SOC 3
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO) 27001, 27017, 27108, 9001
- Department of Defense Security Requirements Guide (SRG)
- Federal Information Security Management Act (FISMA)
- International Traffic in Arms Regulations (ITAR)
- Family Educational Rights and Privacy Act (FERPA)
- Information Security Registered Assessors Program (IRAP) (Australia)
- IT-Grundschutz (Germany)
- Federal Information Processing Standard (FIPS) 140-2

Appendix B. Examples of policy initiatives supporting government cloud adoption

Denmark

Government: Improve efficiency of public sector

Denmark does not have an overarching national strategy for cloud computing, but the technology's potential and importance for the future of the public sector is widely recognized (Daub and Gotfredsen 2019). Cloud solutions are highlighted in various policy initiatives and strategies, such as the Digital Strategy 2016–2020 and the 2018 Digital Growth Strategy. The 2018 Digital Growth Strategy, backed by roughly DKK 1 billion through 2025, focuses on multiple initiatives based on cloud solutions such as Big Data analysis, IoT, and blockchain technologies (Danish Government 2018). On data localization, Denmark follows the framework of the European Union's General Data Protection Regulation (GDPR). Information on Danish citizens is not to be housed outside the European Union, at least for the present, for reasons of data protection.[66]

Public agency: Value for money approach

Ministries and other public sector agencies are encouraged to define their own strategies for the use of cloud solutions and to base their choices on perspectives of security and value for money (Daub and Gotfredsen 2019). Denmark's Digital Strategy 2016–2020 urges public authorities to use the entire spectrum of IT solutions, including cloud solutions, as this can lead to a more efficient and agile public sector while decreasing costs (Danish Ministry of Finance 2016). In mid-2020, the country's digitalization agency published official guidance on cloud computing, concluding that cloud solutions should be implemented on equal terms with traditional solutions.[67]

Israel

Central government cloud infrastructure

As early as 2014, the Israeli government's ICT Authority was instructed to begin transitioning toward a central cloud computing infrastructure for all government ministries and subunits, totaling 51 agencies. The motivations behind the strategy are to reduce operating costs, improve the overall quality of public services, streamline work processes within and between ministries, and to position the

[66] The GDPR imposes restrictions on the storage of personal data outside the EU or its transfer to third-party countries, so as to ensure that the level of protection of afforded individuals by the GDPR is not undermined. Otherwise, the GDPR does not impose any data residency or localization obligations, just as there were no data residency or localization obligations under the GDPR's predecessor, the Data Protection Directive (95/46/EC).

[67] https://digst.dk/media/22430/vejledning-i-anvendelse-af-cloudservices-v11-juli-2020.pdf.

government as a leader in cloud technology in Israel.[68] Despite 2014 resolution and several sets of guidance from the ICT Authority, the Israeli parliament (Knesset) argued in 2019 that implementation at the ministry level still seemed low.[69] According to the then head of the authority, the primary focus in 2019 was to implement public cloud solutions, covering approximately 70 percent of all government activity, while the remaining 30 percent would function via a community or private cloud. A cloud committee headed by the cyber protection unit within the ICT Authority has been established to approve or reject, on a case-by-case basis, public cloud procurements proposed by ministries.

The NIMBUS Project

The main project for transitioning toward the cloud is NIMBUS, a long-term and large-scale flagship project led by several public entities, including the ICT Authority, the National Cyber Directorate, the ministries of finance and defense, and the budget department.[70] NIMBUS will assist in procuring cloud services for the Israeli government to allow it to assert better control over cloud activities and improve public services through digitalization. AWS and Google won the competition to implement the first phase of the NIMBUS project (Solomon 2021). The initial investment is estimated at NIS 4 billion (roughly $1.2 billion).

Moldova

M-Cloud First Policy

The Moldovan government's e-Governance Agency launched its common technology platform, M-Cloud, in 2013, after having established the importance of cloud solutions for the country's future.[71] The M-Cloud First Policy, and the M-Cloud platform, is to be used by the central administrative authorities and other public entities reporting to the government. Public entities are not to create their own cloud infrastructure without the approval of the State Chancellery.

Key reasons for transitioning to the cloud were to reduce government spending on IT services, consolidate data centers in a joint governmental consortium, and improve the quality of public services.[72] In 2017, the World Bank's Independent Evaluation Group found that the M-Cloud had integrated more than 115 data systems across 36 ministries, thus reaching 53.7 percent of central government agencies—well above the targeted 25 percent (World Bank IEG 2017). The M-Cloud brought Moldova international recognition by winning "Best Cloud Project in Central and Eastern Europe" (European Environment Agency 2020).

---

[68] https://www.gov.il/en/Departments/news/cloud_plan.

[69] https://m.knesset.gov.il/EN/activity/mmm/Cloud_computing.pdf

[70] https://www.gov.il/he/departments/news/press_21042021_b.

[71] http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=351760; https://stisc.gov.md/ro/content/mcloud.

[72] https://egov.md/en/projects/m-cloud; https://www.egov.md/en

Nigeria

Cloud First Policy

The Nigerian government launched its Cloud First Policy in 2019 via the National Information Technology Development Agency (NITDA 2019).[73] Under the policy, which is intended to further sustain the country's development and improve the service quality of the public sector, all federal public institutions, as well as public institutions at the state- and local level, are to prioritize cloud-based solutions whenever possible. The policy also applies to companies fully or partially owned by the government. The two main targets of the Cloud First Policy are (i) to increase the adoption of cloud computing among federal public institutions (as well as small and medium-sized enterprises that provide digital services to the government) by 30 percent by 2024; and (ii) to increase overall investment in cloud computing infrastructure by 35 percent, also by 2024. Additionally, it is emphasized that local Nigerian cloud service providers will receive further support to improve their competitiveness—essentially enabling them to operate in the cloud market on equal terms.

Public agency: Cloud solution depends on value for money and specific needs for the individual ministry

The Cloud First Policy states that all public agencies are expected to prioritize cloud services to maximize benefits (NITDA 2019). In practice, when procuring cloud services they are to consider multiple factors such as the value for money; their specific needs for data storage; the risk of vendor lock-in; and impact on finances in the short, medium, and long term. Public, private, and hybrid cloud options are not given *a priori* preference by the Nigerian government; instead, the option chosen should depend on the data sensitivity of each public entity.

Singapore

Commercial Cloud First Policy

Singapore launched its Commercial Cloud First policy in 2018.[74] The policy's main target is to migrate the government's ICT systems to a commercial (i.e., public[75]) cloud option by 2023. The goal is to have at least 70 percent of less-sensitive government systems (e.g., human resources and finance) hosted by the commercial cloud by that time.[76] Prominent arguments for transitioning to the cloud were to improve the availability and quality of public services; lower hosting costs; cut system downtime; sustain economic growth; and increase access to a global ecosystem of solutions and services.[77,78] The government has also created a

[73] https://www.mondaq.com/nigeria/telecoms-mobile-cable-communications/864356/the-nigerian-cloud-computing-policy-digitilisation-of-processes.

[74] https://www.tech.gov.sg/media/technews/soaring-high-with-commercial-cloud.

[75] https://www.bcg.com/publications/2019/economic-impact-public-cloud-apac/singapore.

[76] https://www.tech.gov.sg/files/media/corporate-publications/dgb-public-document_30dec20.pdf.

[77] https://www.csc.gov.sg/articles/digital-government-smart-nation-pursuing-singapore%27s-tech-imperative.

[78] https://www.tech.gov.sg/media/technews/doubling-down-on-cloud-to-deliver-better-government-services.

whole-of-government private cloud, known as G-cloud, as a substitute for public cloud solutions deemed unable to meet security and governance requirements.[79] However, the G-cloud was designed to be compatible with public cloud solutions, thus establishing the opportunity for hybrid solutions.[80]

The Singapore government acknowledges that a one-size-fits all cloud solution does not exist. Therefore, if the individual ministry's or agency's needs cannot be fully met by either public cloud providers or the G-cloud, they are authorized to devise a tailored solution based on a hybrid approach.[81]

United Kingdom

Cloud First Policy

The United Kingdom is pursuing a Cloud First Policy, meaning that all public sector organizations are to consider and evaluate cloud solutions prior to any other options.[82] A main objective is to modernize public services.[83] The policy is mandatory for the central government while being strongly recommended to the broader public sector. Additionally, the Cloud First Policy prioritizes public cloud solutions over community, private, or hybrid options; the reasoning is that public cloud solutions, as a default option, will bring more benefits, both to government entities and end users. The Ministry of Justice has implemented the Cloud First Policy. Its intent is to move all its systems to the public cloud, arguing that it will be able to reduce overall hosting costs by 60 percent in the long run.[84] Although it has left the European Union, the UK continues to follow the Union's GDPR framework with respect to data localization.

Alternatives to cloud solutions

Despite the overarching Cloud First Policy, public departments are free to choose an alternative to a cloud solution or a public cloud solution, but the alternative must offer the right level of security, sufficient flexibility, and a better value for money. Value for money is defined as "securing the best mix of quality and effectiveness for the least outlay over the period of the use of the goods or services bought." [85] It is recognized that a one-size-fits-all cloud solution does not exist, as different ministries deal with different challenges. The ministries are therefore allowed to use solutions other than the public cloud.[86]

---

79 https://www.imda.gov.sg/~/media/imda/files/inner/about%20us/newsroom/speeches/2013/1505_cloudasia2013/gcloudfactsheet.pdf.

80 https://www.bcg.com/publications/2019/economic-impact-public-cloud-apac/singapore.

81 https://www.imda.gov.sg/~/media/imda/files/inner/about%20us/newsroom/speeches/2013/1505_cloudasia2013/gcloudfactsheet.pdf.

82 https://www.gov.uk/guidance/government-cloud-first-policy.

83 https://technology.blog.gov.uk/2019/10/31/cloud-first-is-here-to-stay/.

84 https://mojdigital.blog.gov.uk/2018/10/15/how-were-making-our-hosting-simpler-more-cost-effective-and-more-modern/.

85 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1058990/MPM_Spring_21__without_annexes_040322.pdf.

86 https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector.

Appendix C. Examples of strategic initiatives supporting governmental cloud adoption

Denmark

A one-stop-shop

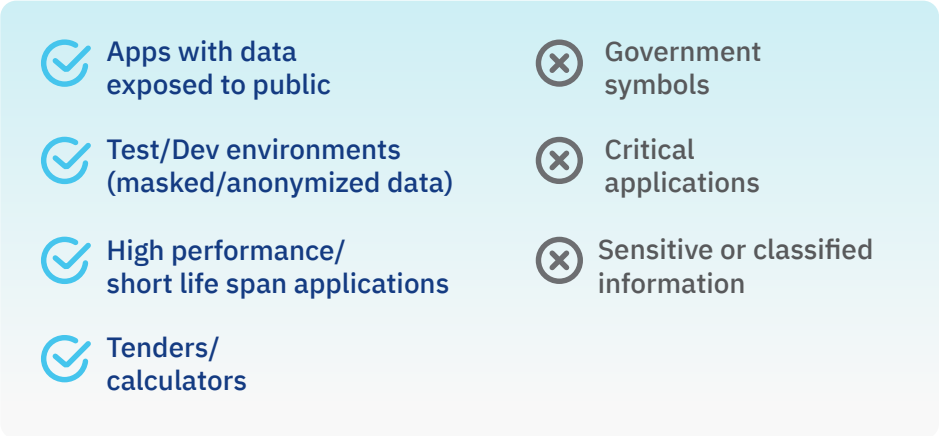
Statens IT is the agency responsible for governmental IT services in Denmark, providing services to 16 ministries and more than 28,000 users. Although Statens IT believes that public cloud solutions will increasingly be used, current on-premise data centers will not be closed, because of their cost-benefit ratio, the data protection they offer, and the potential for vendor lock-in.[87] Overall, the optimal cloud solution hinges on the needs and character of the specific ministry or agency.[88] Public, private, and hybrid cloud options are considered equally feasible solutions (Daub and Gotfredsen 2019).

Israel

Government: A black-and-white list of data types moving to the cloud

Although the Israeli government has not established a definitive data classification scheme, it has established two lists, based on case experience, that identify types of data eligible to be stored on the public cloud (Figure AC.1).

FIGURE AC.1. Types of public data that may or may not be stored in the cloud



Source: https://www.slideshare.net/MosheFerber/goverment-policy-for-public-cloud-case-study-for-the-israeli-goverment.

[87] https://www.computerworld.dk/art/254173/her-er-michael-oernoes-cloud-planer-for-statens-it-du-ser-ikke-os-drage-over-hals-og-hoved-ind-i-noget-cloud.

[88] https://digst.dk/media/22430/vejledning-i-anvendelse-af-cloudservices-v11-juli-2020.pdf.

Nigeria

Government: Establishing a public procurement system and a data classification framework

NITDA, the Bureau for Public Procurement, and other stakeholders are expected to establish a "Digital Marketplace" of pre-approved cloud service providers from which public ministries and agencies can easily procure equipment and services (NITDA 2019). As of June 2021, the marketplace had yet to be launched. To advance the transition toward the cloud, the Nigerian government has developed a data classification framework that public entities, in collaboration with NITDA, can use to categorize their data in terms of sensitivity (Table AC.1). Data in the two least categories are the primary focus of the initial cloud efforts by the ministries and agencies, with each ministry allowed to decide what cloud solution best fits its needs.

TABLE AC.1. Nigeria's data classification system

LEVEL OF DATA SENSITIVITY	CLOUD SOLUTION
National security information	Custom, hardened on-prem systems
Sensitive government business or citizen data	Private and/or hybrid cloud solutions with enhanced security controls
Routine government business	Public cloud solutions with industry standard security
Public or nonconfidential info	

Public agency: Establishing a decision framework for migrating to the cloud

Although the Cloud First Policy was to be implemented immediately in 2019, it includes a one-year grace period followed by a gradual migration to the cloud. During this period, the NITDA developed a decision framework for the cloud migration, which public entities are to follow to create a roadmap for their transition to the cloud (NITDA 2019). The roadmap is set forth in Table AC.2.

TABLE AC.2. Nigeria's roadmap for public agencies' transition to the cloud

SELECT	PROVISION	MANAGE
Identify which IT services to move and when • Identify sources of value for cloud migrations: efficiency, agility, innovation • Determine cloud readiness: security, market availability, government readiness and technology lifecycle.	• Aggregate demand where possible • Ensure interoperability and integration with IT portfolio • Contract effectively to ensure agency needs are met • Realize value by repurposing or decommissioning legacy assets and redeploying freed resources	• Shift IT mindset from assets to services • Build new skill sets as required • Actively monitor SLAs to ensure complaince and continuous improvement • Re-evaluate vendor and service models periodically to maximize benefits and minimize risks

Source: NITDA 2019 (p. 26).

Singapore

Government: Central agencies leading the way

The two agencies driving the government cloud transition in Singapore are the Government Technology Agency (GovTech) and the Smart Nation and Digital Government Office (SNDGO). These agencies receive support from the Infocom Media Development Authority, which consults on the security responsibilities of cloud service providers and sets standards for accountability and transparency.[89]

United Kingdom

Government: Easing public procurement of cloud solutions

Through the UK's Digital Marketplace, ministries, agencies, and other public entities can assess and purchase cloud solutions directly from participating suppliers.[90] This supports the Cloud First Policy for the public sector by easing the procurement process. In 2020/2021 alone, around 80 percent of spending through the marketplace (amounting to £1,78 billion) has originated in the central government. Top spenders include the Home Office, NHS Digital, the ministries of justice and defense, and the Department for Education. Regarding data classification, the UK government has divided its data into three pillars: official, secret, and top secret. Roughly 90 percent of its data are classified as official, which permits a large share of the government's data to be stored in public cloud solutions, reinforcing the Cloud First Policy.[91]

Public agency: Assessment of digital infrastructure before moving to the cloud

Before moving all systems to public cloud hosting, the Ministry of Justice did an internal assessment of its digital infrastructure to identify the appropriate tools and techniques for moving data to the cloud. In practice, the infrastructure fell into the three groups described below.

- Retirement infrastructure: Systems no longer able to be operated effectively, chiefly because of outmoded technologies.
- Modernization infrastructure: Systems already in the public cloud but still presenting difficulties related to managing and updating them.
- Cloud native infrastructure: Systems that can be easily managed, updated, and scaled.

From that point onward the systems, specifically those in the retirement infrastructure-group, were either designated for eventual transfer to the cloud or shut down.[92]

---

89 https://www.bcg.com/publications/2019/economic-impact-public-cloud-apac/singapore.

90 https://advice-cloud.co.uk/ultimate-guide-gcloud/.

91 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf.

92 https://mojdigital.blog.gov.uk/2018/10/15/how-were-making-our-hosting-simpler-more-cost-effective-and-more-modern/.

Appendix D. Examples of operational initiatives supporting government cloud adoption

Denmark

Cooperation with EU countries

Denmark became a signatory to the European Cloud Federation in October 2020 along with other EU member states. The focus is on developing the cloud in both the private and public sectors in the EU.[93]

Israel

First ministry to use public cloud services

The Ministry of Tourism was the first Israeli ministry to begin transitioning to the public cloud in 2015 with help from the ICT Authority. Because of its many overseas tourism offices, the ministry decided to use a Microsoft 365 infrastructure providing e-mail, calendar and file sharing services to replace the outdated and relatively limited local mail services. The main reasons for migrating was to increase the quality of services available to representatives stationed abroad, eliminate the need for multiple servers, and decrease the costs of complex and expensive technical support for these services abroad.

In recent times, in particular during the COVID-19 pandemic, there has been a gradual removal of legal barriers that previously prohibited government ministries and other public entities from uploading information to the cloud. Now, the ministry is allowed to conduct full audit processes using a tablet application; other areas, such as procurement and relations with the local tourist industry, are soon expected to transition to the cloud.

Moldova

Government

MPay has become a central government payment system, reducing the time citizens spent lining up to pay their bills.

Various platforms are ensuring cloud progression

Through various other cloud-based platforms, Moldova is sustaining its M-Cloud First Policy. MConnect allows 53 public agencies and ministries to transfer data without having to rely on paper-based documents. MSign handles more than a million signatures each month.[94]

---

[93] https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe.

[94] https://www.worldbank.org/en/results/2020/10/01/changing-the-development-paradigm-in-moldova.

Nigeria

Biannual review

The Cloud First policy is subjected to a biannual review by NITDA to verify its progress throughout the public sector (NITDA 2019).

Singapore

A platform for testing cloud solutions

To support the Cloud First policy, the government created a platform, Singapore Government Tech Stack[95] that allows agencies to build and test different cloud solutions before implementing them.

United Kingdom

Securing the progress of the Cloud First Policy

To ensure a continuous transition to the cloud, the UK government has introduced the Technology Code of Practice, which urges agencies to 'consider using public cloud solutions first as stated in the Cloud First policy.[96] To comply with the code and the Cloud First Policy, public entities are obliged to present their procurement process and have it accepted by the Central Digital and Data Office.[97]

Public agency: Public cloud by hyperscale cloud providers

The Ministry of Justice primarily uses large hyperscale cloud providers as operators for their more than 800 technology systems.[98] The G-cloud's Digital Marketplace transparently discloses the spending of individual public entities, including the Ministry of Justice.[99]

Regarding data localization, the Ministry of Justice does not require "UK-only hosting" or "UK-only services." Subject to thorough security controls, the ministry allows third-party partners to process and store data (including personal data) outside the United Kingdom.[100]

---

[95] https://www.tech.gov.sg/media/technews/doubling-down-on-cloud-to-deliver-better-government-services.

[96] https://www.gov.uk/guidance/the-technology-code-of-practice#use-cloud-first.

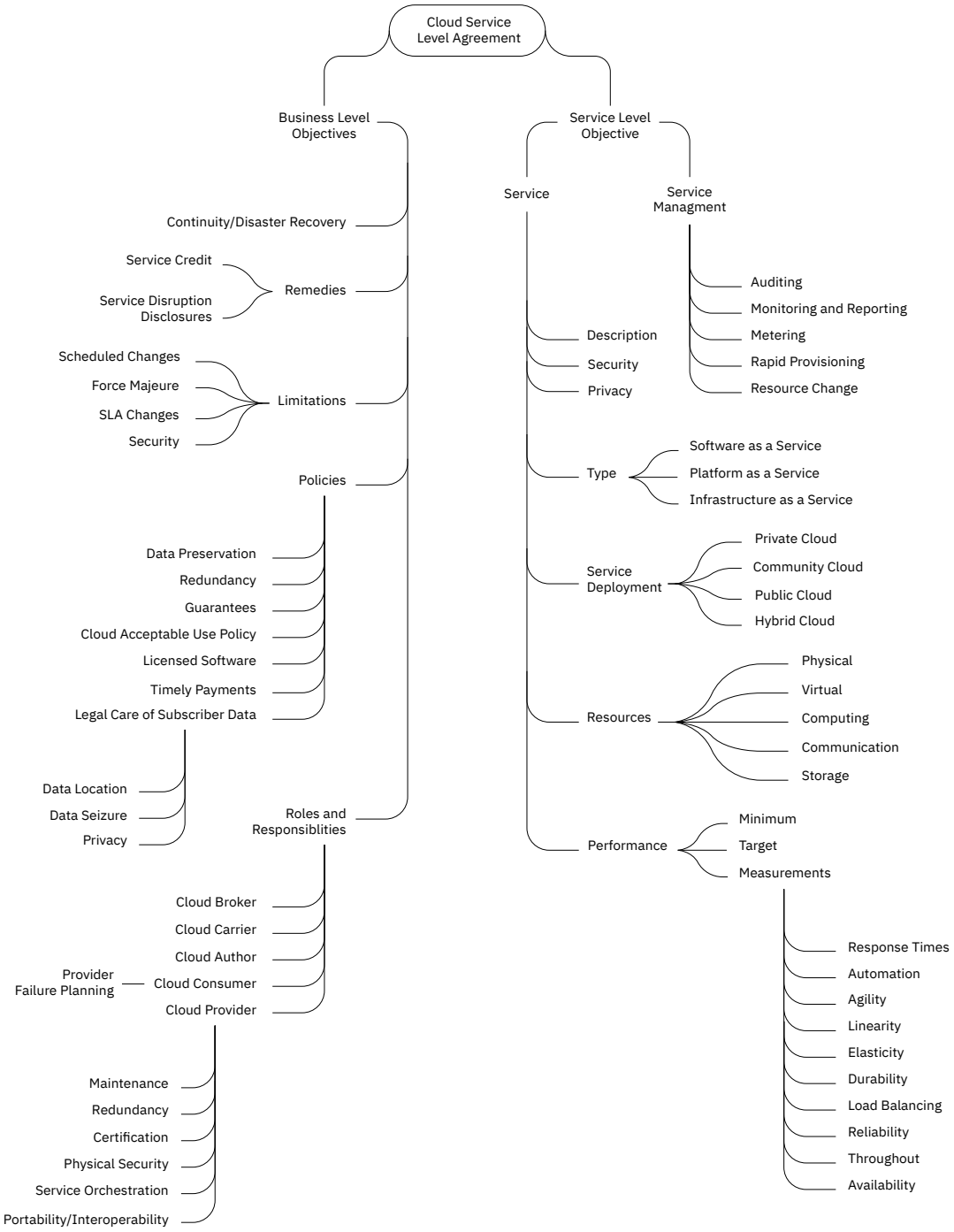
[97] https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service.

[98] https://mojdigital.blog.gov.uk/2019/06/14/security-baseline-in-the-public-cloud/.

[99] https://app.powerbi.com/view?r=eyJrIjoiNTEyMTZhZDAtZGNiNi00OWQxLWI5ODYtMjg1ZWNlMmNkODVhIiwidCI6IjlmOGMwZDc5LTNlODctNGNkMy05Nzk5LWMzNDQzMTQ2ZWE1ZSIsImMiOjh9.

[100] https://security-guidance.service.justice.gov.uk/data-sovereignty/#data-sovereignty.

Appendix E. Sample 'mindmap' structure of a cloud-specific service level agreement (SLA) to facilitate adoption of cloud services



Source: NIST US Government Cloud Computing Technology Roadmap, available at https://www.nist.gov/system/files/documents/itl/cloud/SP_500_293_volumeII.pdf.