CLOUD COMPUTING AS A KEY ENABLER FOR DIGITAL GOVERNMENT ACROSS ASIA AND THE PACIFIC

Thomas Abell, Arndt Husar, and Lim May-Ann

NO. 77

June 2021

ADB SUSTAINABLE DEVELOPMENT WORKING PAPER SERIES

ASIAN DEVELOPMENT BANK

ADB

ADB Sustainable Development Working Paper Series

Cloud Computing as a Key Enabler for Digital Government across Asia and the Pacific

Thomas Abell, Arndt Husar, and Lim May-Ann

No. 77 | June 2021

Thomas Abell is the chief of Asian Development Bank's (ADB) Digital Technology for Development Unit, which is tasked with facilitating the effective use of digital technology to improve development impact. He has over 30 years of professional experience in digital technology.

Arndt Husar is a senior public management specialist (digital transformation) in ADB's Digital Technology for Development Unit, where he facilitates the effective use of digital technology, advising ADB clients, regional departments, as well as sector and thematic groups.

Lim May-Ann is the executive director of the Asia Cloud Computing Association, and managing director of the technology research firm, TRPC Pte Ltd. She is a public policy professional, focusing on development, technology policy, and communications across Asia and the Pacific.

ASIAN DEVELOPMENT BANK

ADB

6 ADB Avenue, Mandaluyong City, 1550 Metro Manila, Philippines
Tel +63 2 8632 4444; Fax +63 2 8636 2444
www.adb.org

Publication Stock No. WPS210196-2
DOI: http://dx.doi.org/10.22617/WPS210196-2

The ADB Sustainable Development Working Paper Series presents data, information, and/or findings from ongoing research and studies to encourage exchange of ideas and elicit comment and feedback about development issues in Asia and the Pacific. Since papers in this series are intended for quick and easy dissemination, the content may or may not be fully edited and may later be modified for final publication.

Corrigenda to ADB publications may be found at http://www.adb.org/publications/corrigenda.

Notes:
In this publication, "$" refers to United States dollars.

ADB recognizes "Kyrgyzstan" as the Kyrgyz Republic, "Korea" and "South Korea" as the Republic of Korea, and "Vietnam" as Viet Nam.

CONTENTS

Tables, Figures, and Boxes		**vi**
Acknowledgments		**vii**
Abbreviations		**viii**
Executive Summary		**ix**
I.	**Background**	**1**
II.	**How Cloud Computing Can Improve Government Services**	**6**
III.	**Barriers and Solutions to Cloud Adoption by Governments**	**9**
IV.	**Recommendations on How Governments Can Effectively Adopt Cloud Computing**	**15**
V.	**Conclusion**	**22**
References		**23**

TABLES, FIGURES, AND BOXES

Tables

1	Data Classification and Government Data	16
2	Government Statements on Data Classification	17

Figures

1	What Is Cloud Computing?	2
2	Cloud Deployment Models	3
3	Example of a Future Career Journey by Deloitte	9
4	Amazon Web Services Pricing Calculator	12
5	Schneider Electric's Data Center Capital Cost Calculator	13
6	Shared Responsibility Model	20

Boxes

1	New Multi-Tier Cloud Security Standard in Singapore	10
2	Steps for Defining the Scope of Cloud Migration	19

ACKNOWLEDGMENTS

This paper was prepared as part of the implementation of the Asian Development Bank (ADB) regional technical assistance, Digital Development Facility for Asia and the Pacific project. Lim May-Ann (domain expert and consultant, ADB) led the writing of the paper, with guidance from Thomas Abell, chief of digital technology for development, Sustainable Development and Climate Change Department (SDCC), and Arndt Husar, senior public management specialist, digital technology for development, SDCC. Samantha Brown (consultant, ADB) copyedited the draft paper; Lawrence Casiraya (consultant, ADB) proofread the draft paper; Ginojesu Pascua (consultant, ADB) prepared the graphics work; and Jennifer Flint (consultant, ADB) typeset and laid out the final publication. Laarni Zapanta-Tuazon, senior operations assistant, SDCC, and Carmela Fernando-Villamar, digital technology officer, SDCC, provided valuable administrative support.

Peer reviewers of this working paper were Marcus Bartley Johns, regional director, Government Affairs and Public Policy (Asia), Microsoft, and Mike Leow, senior compliance manager, Alibaba Cloud (Singapore). ADB greatly acknowledges all these contributions and would like to give special thanks to the Asia Cloud Computing Association and the Amazon Web Services Institute, which provided valuable feedback and inputs.

ABBREVIATIONS

BCDR	business continuity and disaster recovery
CAPEX	capital expenditure
CCOE	cloud center of excellence
COVID-19	coronavirus disease
CBPR	cross-border privacy rules
ICT	information and communications technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	information technology
MTCS	multi-tier cloud security
OPEX	operational expenditure

EXECUTIVE SUMMARY

During a time of accelerated digital transformation and rapid adoption of digital tools, governments are adjusting to the new normal that the coronavirus disease (COVID-19) pandemic has brought about. Internet savvy, digitally connected citizens demand the same level of service from their government as they do from a company that is competing for their business with the latest digital tools. Governments across Asia and the Pacific are responding to change by updating their e-government services, augmenting their data analytics capabilities, and putting in place digital economy development plans.

Many of these changes are enabled by cloud computing technologies, which allow governments to take advantage of the following benefits:

- **Reducing the costs associated with upgrades of legacy technologies**, such as on-premise servers. Adoption requires only one technology migration onto the cloud, which ultimately streamlines the cost of government technology operations and improves overall efficiencies in deploying technology resources. For instance, Singapore's Land Transport Authority reported a 60% in cost savings when moving to cloud from an on-premise solution.
- **Boosting the agility of governments to respond to the needs of citizens and businesses.** For example, a tax department may implement a cloud-based solution that automatically adjusts to system requirements, thereby ensuring the department's ability to respond to demand during peak periods, such as tax return deadlines.
- **Improving public sector resilience and recovery capabilities in times of crisis**, such as the COVID-19 pandemic. The Ministry of Education of the People's Republic of China, for instance, was able to set up a national cloud-based education platform in record time, allowing students to continue their studies during movement control lockdowns.
- **Ensuring that public sector human resources keep up with technology development.** Building public sector solutions with the latest cloud computing resources and tools ensures that governments keep up with other sectors. Attracting and retaining technology talents who want to serve in the public sector is essential if a government wants to retain in-house capabilities. Having to maintain an aging or outdated technology platform is demotivating and will accelerate a decline in service quality compared to that of other sectors.

However, the adoption of cloud computing still faces barriers in the public sector. In the first instance, it remains a challenge for policy makers to establish security and data protection policies that balance the need to protect data with the need to enable secure data flows. Some governments have put in place restrictive regulation (e.g., data localization). Others have developed multiple technical and security policies which overlap with existing international standards, creating a complex mesh of conflicting policies.

Other barriers to cloud adoption are outdated cost structures and public procurement modalities. In many cases, government agencies may want to purchase cloud services, but the existing purchasing rules may not allow utility-based variable cost items, such as cloud services, to be purchased. Updating such policies may require legislative changes, which would take significant time to be proposed and passed officially.

There are also technical barriers for the adoption of cloud computing, as technical knowledge of the specific requirements in the public sector is required to begin the system design and cost-estimation

processes. In some instances, personnel may not be available and external resources may need to be brought in.

Apart from these barriers to adoption, governments need to manage the vendor concentration risk (i.e., relying on a single or a small number of vendors) which is typical for digital technology projects. Given that cloud computing relies on stable internet connectivity, it should be a key consideration for adoption, and a determinant of the configuration that is eventually chosen.

This paper offers three recommendations on how governments should start to adjust their policies to enable greater cloud adoption:

First, governments should **establish a conducive regulatory environment** that supports the adoption of cloud computing in the public sector. This could include:

- Limiting data localization policies that might be in place.
- Establishing cross-border data transfer mechanisms.
- Implementing a data classification framework that allows for different types of data to be managed differently.
- Creating an interoperable cloud system for government. This may benefit from an iterative policy process where adjustments and harmonization can be negotiated in the case of conflicting policies.

Second, governments should **establish a clear and robust cloud strategy and adoption plan**. This would include details on their intended migration and/or implementation approach, underpinned by an overarching government cloud policy.

Finally, governments should **ensure that in-house support is provided** to guide government institutions on their journey of adoption. This could be achieved through the designation or creation of a dedicated unit or center of excellence, as well as a cloud procurement marketplace that would allow fast and safe assessment and purchase of cloud services for public sector deployment.

I. BACKGROUND

As citizens and businesses consume more digital content and become increasingly reliant on digital sources for information and services, governments are also adapting to the rapid changes in digital usage and consumption patterns. For example, many governments have now seen the importance of ensuring that citizen services are available online, and have worked to improve their e-government efforts, as documented longitudinally by the United Nations' e-Government Survey.[1] Many ADB developing member countries have launched initiatives to digitally transform their governments, such as the Government of Tajikistan's Digital Economy 2040 Concept and Digital CASA Tajikistan Project,[2] the Government of Viet Nam's announcement of their National Digital Transformation Programme 2020–2025,[3] and the Government of the Kyrgyz Republic's Digital Kyrgyzstan 2019–2023.[4] Yet other governments have announced long-term strategies to develop their country into smart nations, such as the Government of India's 2015 commitment to build 100 smart cities.[5]

One of the key enablers for these transitions is cloud computing technology, which enables ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (Figure 1). Cloud computing offers a means for digital government services to be delivered in a more agile, faster, and cheaper manner compared with traditional information technology (IT) infrastructure. Yet changing course and introducing a new paradigm for information and communications technology (ICT) infrastructure comes with strong disincentives. Over decades, governments have invested heavily in on-premise data centers and their accompanying technology architecture (i.e. servers, cooling systems, hardware and software upgrades) as well as the operation and maintenance of hardware and software, etc. This legacy infrastructure means there will be resistance to moving to cloud computing, such as:

- The infrastructure investment may not have reached its financial accounting "end of life" yet, due to an accounting system that amortizes and writes off such capital costs over a period of time.
- Existing staff capabilities and capacities may not be ready for a migration into a new system; there may possibly be a need to reorganize headcount, and/or retrain staff to use the new systems.
- Government and system policies may need to be overhauled in order to move to cloud computing. This may include redesigning database systems, instituting technical interoperability policies, developing cloud governance mechanisms, and adjusting public sector procurement policies—all of which may require time and possibly legislative changes to put in place.

Cloud computing is increasingly recognized as a core technological building block for digital innovation. Moving government systems into a cloud environment and integrating its full capabilities into new digital solutions can help future-proof the public service. The move from on-premise solutions toward cloud solutions ("cloud deployment") can be a gradual process and different options are available, including private cloud, hybrid cloud, and public cloud deployments (Figure 2). Software-as-a-service applications such as citizen-centric mobile apps may be built and delivered for the public, and government engineers using platform-as-a-service may securely share source code together, greatly reducing the duplication of programming resources.

---

1 United Nations. 2020. *United Nations e-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development.*

2 *Smart Energy International.* 2020. Tajikistan's Digital Transformation Wins Korea and World Bank Support. 6 February.

3 S. Dharmaraj. 2020. Vietnam Aims to Become a Digital Society by 2030. *Open Gov Asia.* 8 June.

4 *24.KG.* 2018. Kyrgyzstan Develops Concept of Digital Transformation. 14 December.

5 S. Wray (ed). 2020. India Pledges Five More Smart Cities. *Smart Cities World.* 3 February.

Figure 1: What Is Cloud Computing?

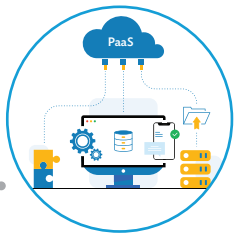
Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Examples – Slack, Trello, Office 365, Salesforce, Dropbox
Users - End-users

What is Cloud Computing?

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



Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Examples – Cloud Foundry, Heroku, Github, Kubernetes, Docker
Users - Software developers and engineers

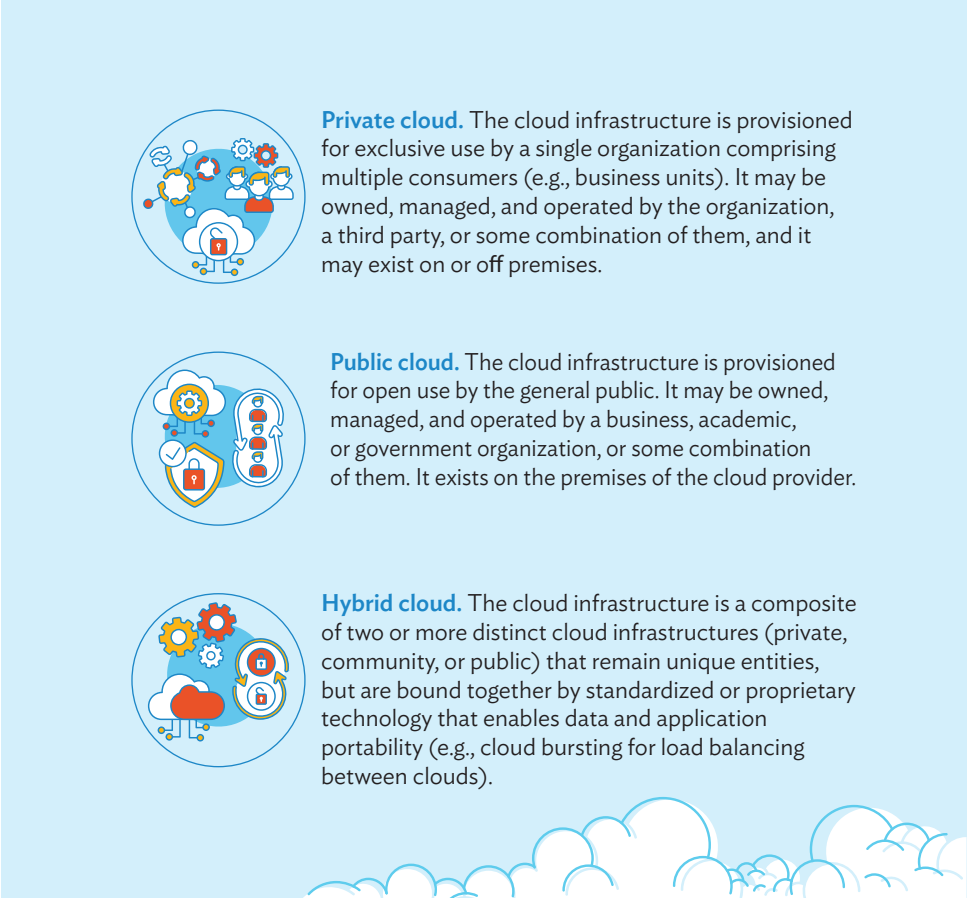
Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Examples – AWS, Google Cloud Platform, Azure, VMware, OpenStack
Users - Network architects and tech administrators

Source: Adapted from P. Mell and T. Grance. 2011. *The National Institute of Standards and Technology Definition of Cloud Computing: Recommendations*.

Figure 2: Cloud Deployment Models



Source: Adapted from P. Mell and T. Grance. 2011. *The National Institute of Standards and Technology Definition of Cloud Computing: Recommendations.*

A. Benefits of Cloud Computing for Governments

Cloud computing **reduces the cost of purchasing, setting up, and running and maintaining technology services.** Cloud computing offers governments the opportunity to streamline technology operations, and greatly improve efficiency, particularly reflected in the time it takes to process citizen-facing transactions.

Cloud computing also **allows governments to respond in an agile manner** to citizen requirements, and allows public services to scale, where required, for instance, in cases where services may face peak demand periods, such as filing online tax returns just before a deadline. Using cloud computing allows governments to handle demand spikes without service interruptions, as technology support is scaled as required.

Similarly, cloud computing **improves government resilience and offers business continuity and disaster recovery services** where there might be outages caused by a natural disaster, or if other adverse events impact a country. Cloud computing increases government resilience to cybersecurity threats, as in many cases moving to cloud offers stronger cybersecurity and privacy capabilities and protections (such as security engineers, intelligence and threat monitoring systems), which they may otherwise find difficult to resource and keep updated.

Cloud computing also allows governments to **achieve better technological and analytical capabilities**. Otherwise, they may struggle to access, for example, artificial intelligence and machine learning, which offer supercomputing power for large-scale data processing and analytic capabilities.

Finally, a move to cloud computing helps **facilitate human resource development paths** in the public sector, and also helps future-proof government infrastructure, as moving to the cloud requires all technology professionals to keep up to date with the latest equipment and software, rather than focus on maintaining aging technology platforms.

B. Cloud First and Whole-of-Government Approaches

There are many benefits to moving to cloud computing in the public sector, and thus many governments have introduced cloud-first policies. These are policies mandating that government agencies and departments prioritize the use and procurement of cloud systems by default where a secure, reliable, and cost-effective cloud computing option exists.

In many instances, the introduction of a cloud-first policy also heralds a new whole-of-government approach toward technological policy making, where governments revisit the manner in which government services are administered.

For example, in **Australia**, the Australian Signals Directorate was originally the certification authority for public sector agencies wanting to use cloud computing. From 2 March 2020, the Australian government revised this scheme in favor of a new cloud security guidance document, with technology guidelines and standards that support the secure adoption of cloud services across government and industry.[6]

In October 2016, **Singapore** established its government technology agency, GovTech, to consolidate previously distributed functions and to oversee the overall digital transformation of its public sector. GovTech comes under the Prime Minister's Office, services all line ministries and statutory boards in their digital transformation journeys, and is the implementing agency for the Smart Nation agenda.[7] Among the efforts by GovTech to establish a digitally enabled government is the establishment of the Singapore Government Tech Stack.[8] This is a stack that hosts a suite of tools and services on the Next-Generation Container Architecture cloud platform-as-a-service, which allows government developers to create and share their applications and services with other government agencies on a secure platform. Services developed are made interoperable with other government services through the use of a centralized government-wide application programming interface exchange, APEX. This serves as a searchable library of application programming interfaces for developers to draw code from.[9]

C. Trending Cloud Computing Developments Within the Government Sector

Nowadays, citizens expect their government to provide services, disseminate information, and engage them via digital means. Public sector reforms tend to leverage technology to fundamentally transform the way government operates and delivers services. When the private sector transforms faster, the expectations of citizens in regard to their level of service challenge public institutions to deliver faster,

---

6 Australian Cybersecurity Centre. 2020. *Cloud Services*.
7 I. Tham. 2020. GovTech Launched to Lead Digital Transformation in Public Sector. *The Straits Times*. 27 July.
8 GovTech Singapore. n.d. *Singapore Government Tech Stack*.
9 *GovTech Singapore*. 2018. Getting to Know NECTAR and APEX. 24 July.

higher quality, and better services. In recent years, many governments have embarked on digital transformation journeys, involving the digitalization of many citizen- and corporate-facing services and the adoption of foundational technologies such as digital identification systems, national database management systems, and digital payment platforms.

Efforts in pursuit of sustainability targets, such as the United Nations Sustainable Development Goals, usually integrate digital technology solutions that help accelerate progress and augment impact. The following examples for the environmental sector (clean tech), food and water security (agritech), financial sector (fintech), and health sector (health tech) usually build on research and development that has been subsidized and/or enjoys direct investment from or business dealings with public agencies.

Clean tech are technologies that allow for economic growth in a sustainable way. The World Economic Forum estimates that 2019 investment in the sector was worth more than $300 billion.[10] An increasing awareness of the global plastic problem is driving many young citizens to use their knowledge of technology to solve environmental issues. For instance, students from **Viet Nam** designed a floating trash collector to clean up plastic waste at the beach and at sea.[11]

Agritech are technologies that explore technical solutions to food security. Some estimates pegged 2019 global investment in this sector at $19.8 billion.[12] An example of agritech deployment by the public sector is the Republican State Enterprise Kazvodkhoz, a state-owned enterprise in **Kazakhstan**, which is currently building an irrigation project to rehabilitate 171,000 hectares of land in the country to improve its agricultural productivity and promote the diversification of agricultural products. This means shifting from traditional low-yield and low-value crops into high-value cash crops. Four provinces fall under the project: East Kazakhstan, Karaghandy, Kyzylorda, and Zhambyl. In particular, the project is piloting an irrigation monitoring system using remote sensing technologies.[13]

Fintech are technologies deployed to develop new financial services, with some estimating that global fintech funding was worth $24.6 billion in 2019, with strong potential for growth (footnote 12). An example in the public sector would be the Monetary Authority of **Singapore**'s announcement that it would deploy Open Banking, enabling Singaporeans to view all their bank statements and investments on a single platform.[14]

Health tech are deployed to better manage and allow citizens to self-monitor their health. For example, the **Republic of Korea** developed the Epidemic Investigation Support System in response to the need to conduct movement and contact tracing during the COVID-19 pandemic.[15]

This paper explores how cloud computing is supporting digital transformation in the public sector and examines what must be done to help governments effectively utilise it, promote its greater adoption in the private sector, and realize its benefits for its own operations and the broader economy.

---

10 S. Kivity. 2020. 3 Hard-Won Lessons from a Decade of Negative Cleantech Returns. *World Economic Forum*. 13 March.
11 *Viet Nam Net Global*. 2019. Young Students Design Made-in-Da Nang Trash Collector. 17 June.
12 *Mastercard*. 2020. FinTech in 2020: Five Global Trends to Watch (CB Insights in Partnership with Mastercard Start Path). January.
13 ADB. 2019. ADB-Supported Irrigation Project to Improve Kazakhstan's Agricultural Productivity. News release. 11 September.
14 G. Ho. 2020. Singaporeans Can Soon View their Bank Accounts and Investments on a Single Platform. *The Straits Times*. 1 December.
15 H. Shin et al. 2020. How South Korea Turned an Urban Planning System into a Virus Tracking Database. *Reuters.* 22 May.

II. HOW CLOUD COMPUTING CAN IMPROVE GOVERNMENT SERVICES

A. Cloud Computing Reduces Costs

One of the most widely recognized benefits of cloud computing is its economies of scale. Instead of having to invest heavily in data centers and servers with limited advance knowledge of their eventual usage, cloud allows users to only pay for computing resources that are consumed. Users are able to swap capital expense for variable operational expense.

In addition, governments can achieve more control over their variable costs than they can by operating their own infrastructure, often achieving a lower aggregate cost with multi-tenant efficiency across many government agencies hosted in a GovCloud.[16] This enables service providers to achieve higher economies of scale that translate into lower pay-as-you-go prices.

By reducing staffing as well as operations and maintenance expenditure for data centers, governments are also able to shift their focus toward improving citizen-facing services.

Singapore's Land Transport Authority, which decided to use cloud computing for web hosting instead of building their own data center, experienced cost savings of 60% when compared to on-premises infrastructure.[17]

In the **Philippines**, the Bureau of Customs estimated that it would need to spend about ₱200 million ($4.17 million in 2016) to rehabilitate its aging internal data center, whereas if it used cloud computing infrastructure, it would have the computing power required for less than one-tenth the cost.[18]

B. Cloud Computing Streamlines Operations and Improves Efficiency

Using cloud-based tools allows governments to reduce processes and streamline operations. Cloud platforms give governments access to productivity tools that they can use to consolidate administrative and operational processes, and remotely exchange information among multiple stakeholders.

This not only gives a better overview of existing processes, which can improve workflow management and identify roadblocks, but also creates a pool of data that can be used to glean insights for future decision-making, monitoring, and evaluation of government services.

The **Philippines**' Department of Information and Communications Technology in 2017 used a cloud-based solution to automate its business permits and licensing system, enabling local government units to process business permit applications and renewals online, reducing the duration of the process from 2–3 days to a range of just 30 minutes to half a day.[19]

In the Australian state of South **Australia**, the Department for Communities and Social Inclusion was able to deploy a single platform and automated contract administration and processing of payments

[16] R. Harms and M. Yarmartino. 2010. *The Economics of the Cloud*.
[17] Amazon Web Services. 2016. *Land Transport Authority of Singapore Case Study*.
[18] Amazon Web Services. 2016. *Bureau of Customs of the Philippines Case Study*.
[19] *Microsoft. 2020*. Philippine Government Automates Business Permits and Licensing System. 30 April.

to nongovernment organizations using a software-as-a-service cloud platform, reducing payment processing time from 4–6 weeks to less than 3 days.[20]

Further, cloud computing is also a foundation for emerging technologies such as artificial intelligence and virtual reality, which are helping organizations realize productivity and efficiency gains. Governments looking into developing smart cities and innovative virtual solutions for existing problems may leverage the use of these technologies on the cloud.

Thailand's Ministry of Public Health is able to identify public health risks and disease hotspots to mitigate the risk of epidemics through a cloud-based artificial intelligence analytics using data that is recorded, tracked, and shared through a mobile application. With an accuracy rate of 80%–90%, the artificial intelligence model identifies the conditions of public restrooms through volunteer-submitted photos of restroom hygiene and notifies local restroom operations staff of specific sanitation issues that need to be resolved.[21]

C. Cloud Improves Agility and Allows Public Services to Scale

In a cloud computing environment, software solutions, data storage, and computational capacity can be deployed with a few clicks on a mouse, making government agencies highly nimble in adjusting to citizen needs. In comparison to traditional ICT infrastructure, the deployment of ICT resources is reduced from weeks to just minutes. Cloud computing has even fostered a new collaborative approach to ICT services called DevOps, where development and operations are combined into a continuous activity, resulting in faster cycles of development and improvement.

Furthermore, because cloud computing is a measured service charged on a per-use basis, governments no longer need to speculate on their future infrastructure and capacity needs. Government agencies can access as many or as few resources as needed and scale up and down as required with only a few minutes' notice. Moving to cloud therefore avoids redundancy, where governments may over-purchase computing resources that wind up idle or face resource crunch when traffic peaks.

In 2016, **Azerbaijan** established its first ever Tier III data center in the Caucasus region, and with its development in Baku, the country hopes to scale up into a regional information transit center.[22]

The Ministry of Education in the **People's Republic of China** developed a national cloud-based education platform that allowed students to continue their studies during the COVID-19 lockdowns. Two months after its launch in February 2020, 270 million students had accessed online classes via the platform.[23]

Through the use of cloud-based collaborative tools, **Japan**'s Osaka City government was able to smoothly transition 2,000 employees to telework at the start of the COVID-19 city-wide lockdowns in March 2020.[24] This transition was part of the "Osaka City ICT Strategy 2nd Edition" action plan, which included "Telework Implementation Guidelines" to be established in 2018, but it had seen limited implementation until the COVID-19 crisis. This immediate shift to telework due to movement restrictions for these 2,000 employees (representing 10% of all government agency employees in the city) was significant not only because it represented a large number of government employees, but also because the shift was immediately implementable, thanks to an earlier cloud migration into Microsoft Office 365.

---

20 Salesforce. n.d. *Cloud Adoption in Government: Salesforce Drives DCSI Service Innovation to Improve the Lives of People with Disabilities*.

21 *Microsoft*. 2019. Thailand's AI-Powered Healthcare System Curbs Government Costs, Helps Save Lives. 26 April.

22 Azerbaijan Council. 2019. *Digital Bridge between Europe and Asia, 2019–2022*.

23 Q. Xu. 2020. Planning for Lockdown and How to Emerge Out of It. *University World News*. 25 April.

24 *Microsoft*. 2020. City Government of Osaka. 16 September.

D. Cloud Improves Resilience with Better Business Continuity and Disaster Recovery

The benefits of the cloud in relation to business continuity and disaster recovery (BCDR) is not limited to capital expenditure (CAPEX) savings. Using the cloud can improve resilience through customized BCDR mechanisms that can distribute and/or replicate data and workloads across multiple data centers in disparate geographic locations on a near real-time basis. This helps governments mitigate against geographically concentrated risks, without the cost and complexities of operating multiple data centers themselves.

The Australian state of Western **Australia**'s land information authority, Landgate, was able to minimize the effect of a severe storm resulting in a power outage on its land titles system, a critical system that allows users to register and search for land titles, due to advanced cloud features that allowed for the cost-effective implementation of BCDR measures.[25] Thanks to their decision to move to the cloud, the system was only impacted by the power outage by 4–5 minutes before the BCDR system kicked in with a database fail-over system automatically being established.

Azerbaijan's Heydar Aliyev International Airport in Baku has moved to using cloud technologies for all of its databases, digital resources, and systems for displaying flight information.[26] As part of an upgrade of its database and resource management systems under Amadeus, it is also implementing the Amadeus Altéa Passenger Service System software, which gives the airport the full benefit of cloud computing, providing the airport with strong fail-over capabilities in times of emergency or crisis, as applied to its business needs, such as reservation, inventory and departure control capabilities.

E. Cloud Facilitates Human Resource Development

Cloud not only enables in-house developers to be more productive by shifting development teams from legacy platforms to a state-of-the-art development platform where they have industry-leading tools and services at their disposal, but also improves talent acquisition and retention within a highly competitive sector.

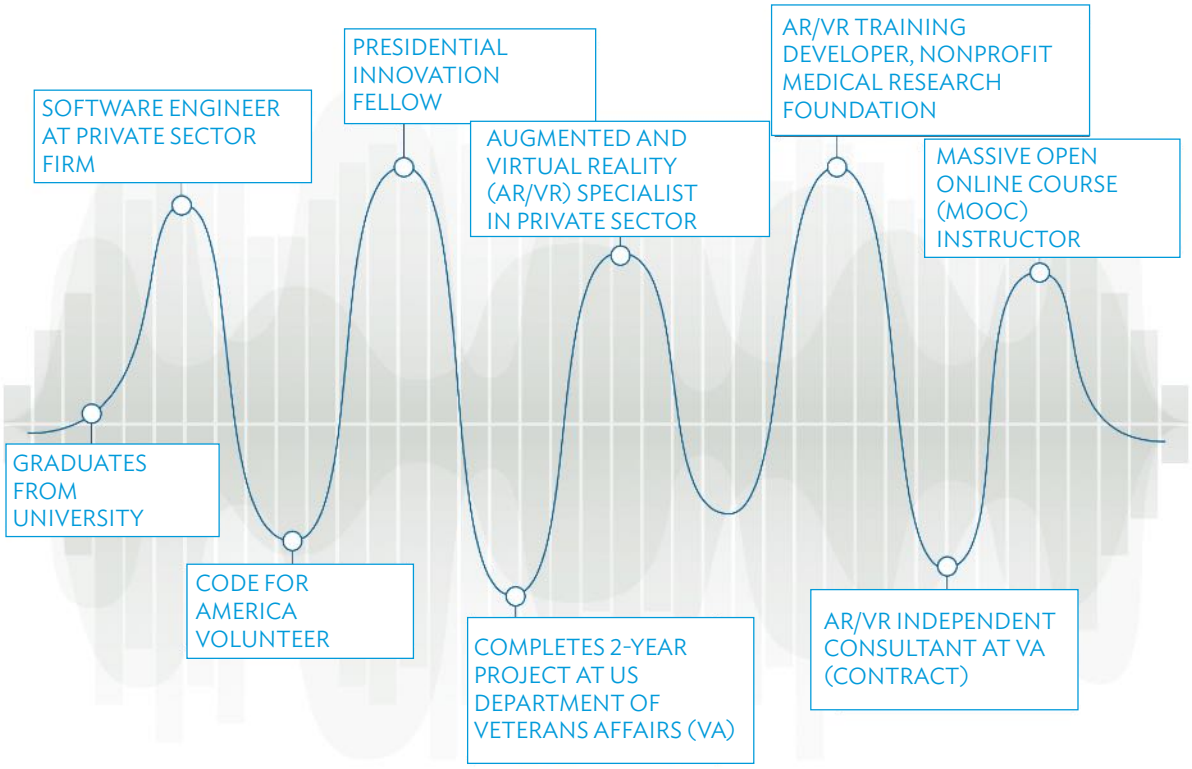
Developing and maintaining excellence in digital service, and keeping up with technology advancement, will attract leading computer and network engineers and architects into government careers, rather than a continuation of the situation in which governments have difficulty attracting top talent into jobs that are focused on maintaining aging technology platforms.

For example, some United States (US) government IT systems are more than 20 years old and are written in outmoded programming languages such as COBOL.[27] Not only will this legacy infrastructure be difficult to support, but it also prevents governments from transiting to a new model for career journeys, such as a possible "tour of duty" approach toward future careers, put forth by Deloitte in Figure 3.

---

[25] *Western Australian Government–Office of Digital Government*. 2019. Landgate–Cloud Transition Case Study. 1 February.
[26] Y. Kazimbeyli. 2019. Azerbaijan's Largest Airport Pioneers Cloud Computing. *Caspian News*. 5 July.
[27] B. Robinson. 2020. Legacy Systems: Too Old to Die? *GCN: The Technology that Drives Government IT*. 16 April.

Figure 3: Example of a Future Career Journey by Deloitte



Source: W. Eggers et al. 2019. The Future of Work in Government: Navigating a Shifting Talent Landscape. *Deloitte*. 28 February.

III. BARRIERS AND SOLUTIONS TO CLOUD ADOPTION BY GOVERNMENTS

A. Lack of Processes for Data Protection and Security

It can be challenging for some government officials to fully grasp the way data protection and security works in a cloud environment, given prevailing misconceptions around what constitutes security and data protection. Some believe that outsourcing IT infrastructure and systems means that they have to relinquish control over their security and data protection processes, and that this may increase risks. This is not true, because security solutions may be more robustly implemented and imposed on a system-wide basis with cloud computing.

A number of governments, particularly those of large economies, have also reached the conservative conclusion that data must be hosted within their national borders to maintain security, a concept called "data localization." However, in a cloud context, security is reliant on the specific measures that the customer decides to implement, as customers ultimately have full control and ownership over their data. For example, a customer may decide to share his or her account password with another person, who then breaches the customer's trust and absconds with a sum of money. In this case, a better preventive security measure could not have been implemented, even if the data was stored within the country.

Another common misconception is that cloud providers have full access to the data that is hosted on their platforms and can be prevailed upon to provide governments with access to user-hosted data. In fact, most cloud computing security policies now include strong encryption keys which customers maintain to safeguard their data against any unwanted or unwarranted access. The cloud provider has no way to access the data hosted on their platforms, as any encrypted data would effectively be rendered useless without the applicable decryption keys.

➢ Solution: Cloud Security Certifications

One approach toward improving data protection and security is to mandate a security certification for government cloud computing.

To help agencies better recognize security adequacy and confidently approach cloud computing, the Government of **Singapore** in October 2013 launched the world's first cloud security standard covering multiple tiers of cloud security—the Multi-Tier Cloud Security (MTCS) Standard for Singapore.[28] As of October 2020, there were 112 MTCS-certified cloud services, of which 19 were software as a service.[29] The MTCS covers three tiers of security, with Tier 1 being the base level of security, and Tier 3 being the most stringent (Box 1).[30]

Box 1: New Multi-Tier Cloud Security Standard in Singapore

Tier 1: Designed for non-business critical data and systems, with baseline security controls to address security risks and threats in potentially low-impact information systems using cloud services (e.g., a website hosting public information).

Tier 2: Designed to address the needs of most organizations running business-critical data and systems through a set of more stringent security controls to address security risks and threats in potentially moderate impact information systems using cloud services to protect business and personal information (e.g., confidential business data, email, customer relations management systems).

Tier 3: Designed for regulated organizations with specific requirements and more stringent security needs. Industry specific regulations may be applied in addition to these controls to supplement and address security risks and threats in high impact information systems using cloud services (e.g., highly confidential business data, financial records, medical records).

Source: Infocomm Development Authority of Singapore. 2013. *New Multi-Tier Cloud Security Standard in Singapore*. 13 November.

However, there are challenges to developing and maintaining a national technical standard for cloud computing, as national standards often duplicate the work on industry standards which are discussed in multi-stakeholder forums such as the International Organisation for Standardization (ISO), the International Electrotechnical Commission (IEC), and other similar platforms. To prevent fragmentation of the technology security system, governments have chosen to adhere to international data protection and security standards in their cloud certification frameworks.

[28] Infocomm Media Development Authority of Singapore. 2020. *Cloud Computing and Services*. 10 December.
[29] Infocomm Media Development Authority of Singapore. 2021. *Compliance and Certification*. 7 January.
[30] Infocomm Development Authority of Singapore. 2013. *New Multi-Tier Cloud Security Standard in Singapore.* 13 November.

Singapore's MTCS standard was built upon ISO 27001[31] while **Japan**'s Information System Security Management and Assessment Program management standards are based on ISO/IEC 27001 and ISO/IEC 27002 on information security[32] and ISO/IEC 27017[33] on information security of cloud services.

In order to fully capitalize on the advantages of cloud computing, governments need to improve their understanding of the security provisions as well as available solutions for data protection risk management.

B. Poor Understanding of Cloud Cost Structures and the Utility Procurement Model

Governments generally operate older, legacy solutions due to public sector budgeting and investment norms.

Global consultancy firm Deloitte reports that governments that moved to the cloud saved as much as $2 billion over 5 years.[34] However, this benefit is at times overlooked or downplayed in favor of the ease and comfort of continuing with existing legacy solutions. Consequently, much of governments' IT budgets go toward sustaining basic systems and legacy infrastructure, leaving few resources for innovation and the adoption of emerging technologies. The cost associated with migrating systems to the cloud is a particularly large challenge for public sector agencies.

Government procurement processes are geared toward a capital expenditure one-time procurement of hardware, software licenses, and consulting, but are not typically adept at acquiring cloud services which are designed as operational expenditures.

Because government procurement processes are geared toward the procurement of hardware, software licenses and consulting (CAPEX), current procurement criteria are not suitable for purchasing cloud services, where costs accrue over time (operational expenditure or OPEX). Cloud utility (pay-as-you-go) pricing models significantly differ from the traditional cost structure of ICTs which is based on a pay-once model. In this situation, entrenched government costing practices are a barrier to cloud adoption.

Government IT departments are not skilled at estimating the implementation or operating costs of cloud services. These services evolve rapidly, too, so this knowledge is difficult to keep current.

In some cases, the variable nature of the cost of cloud services, and the highly technical nature of cloud cost estimations, can be a substantial barrier for a government to move to cloud, despite offering lower lifecycle costs.

For example, cloud pricing calculators set up by cloud companies often request information from users, such as getting them to select products, estimate scenarios for usage such as "size of request

---

31 *Microsoft*. 2020. Multi-Tier Cloud Security Standard for Singapore. 1 January.

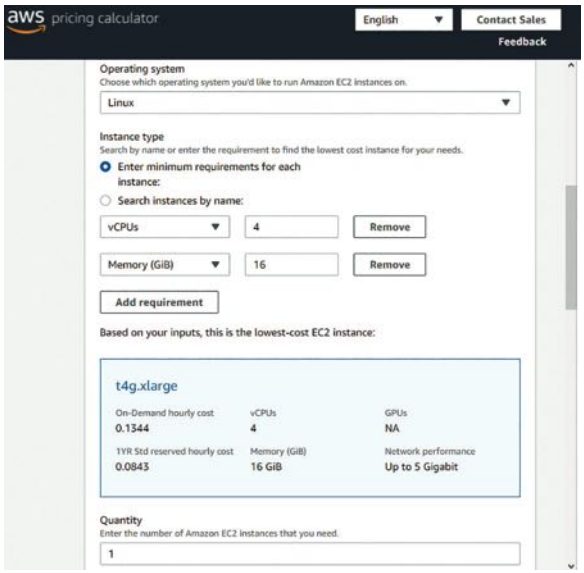
32 ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. These requirements are generic and are intended to be applicable to all organizations, regardless of type, size, or nature. ISO/IEC 27002 provides guidelines for organizational information security standards and information security management practices including the selection, implementation, and management of controls taking into consideration the organization's information security risk environment(s). Source: ISO. 2018. *ISO/IEC 27000: Key International Standard for Information Security Revised*.

33 ISO. 2015. *ISO/IEC 27017: Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

34 Deloitte. 2019. Harnessing Public Cloud Opportunities in the Government Sector. *Access Economics*. 22 March.

(in kilobytes)," number of request units per month, or if selecting for computer facilities, to estimate the required instances for virtual central processing units or graphics processing units (Figure 4).[35] These technical details may elude the average government official, unless they are specialists in cloud computing. Hence, it is better to estimate costs by consulting with potential vendors on various scenarios for cloud computing use, particularly if larger projects are concerned.

Figure 4: Amazon Web Services Pricing Calculator



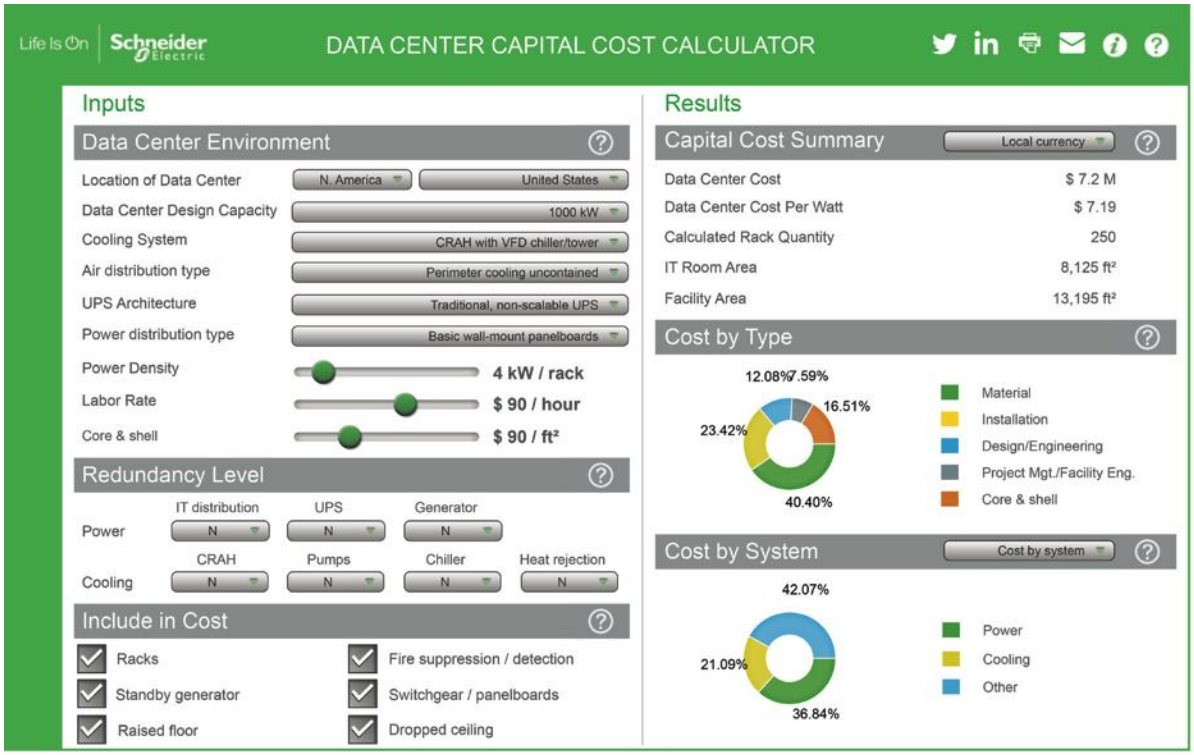
Source: Amazon Web Services. Amazon Web Services Pricing Calculator. https://calculator.aws/#/createCalculator/EC2

Another example of a more in-depth cloud cost estimation—for example, building a government data center—can be seen in the screenshot below of Schneider's Data Center Capital Cost Calculator, which requires a very detailed understanding of technical requirements such as data center design capacity, cooling systems, power density, labor rates, core and shell requirements, racks, etc. (Figure 5).

In **Australia**, the biggest practical difficulty government agencies faced in adopting cloud was in re-classifying IT budgets from CAPEX to OPEX. While agencies typically have annual IT capital budgets, operational budgets are shared across departments. This makes it unclear where the operational costs for cloud can be charged, as IT is normally assumed to have been budgeted as CAPEX. This means that IT departments would have to compete with other operational activities within the agency to increase their operational budgets, leading to budget cuts in other areas, while CAPEX budgets remain under-used. An additional challenge was the common perception that shifting to new OPEX models resulted in more long-term uncertainties compared to the CAPEX model (footnote 34).

[35] See Microsoft Azure. Pricing Calculator. https://azure.microsoft.com/en-us/pricing/calculator/; Amazon Web Services. Amazon Web Services Pricing Calculator. https://calculator.aws/#/createCalculator/EC2; Google. Google Cloud Pricing Calculator. https://cloud.google.com/products/calculator; Huawei Cloud. Elastic Cloud Service Price Calculator. https://www.huaweicloud.com/intl/en-us/pricing/#/ecs; Alibaba Cloud. Elastic Compute Services (Subscription) Price Calculator. https://www.alibabacloud.com/pricing-calculator#/add/acm-195b9957-d5b9-41ae-9ae2-b0903fd802fd/vm_intl/vm_intl

Figure 5: Schneider Electric's Data Center Capital Cost Calculator



Source: Schneider Electric. Data Center Capital Cost Calculator. https://www.se.com/ww/en/work/solutions/system/s1/data-center-and-network-systems/trade-off-tools/data-center-capital-cost-calculator/

➢ **Solution: Move public sector from capital expenditure single-expenditure to operational expenditure utility-based procurement model.**

To address such difficulties, government agencies must ensure that chief financial officers and finance departments understand how cloud adoption may require updated procurement rules and processes that would shift IT expenditures from capital to operating expenditures. This could start with a perception shift to message to the relevant government staff that cloud purchasing is a new model of purchasing technological resources as a utility (i.e., OPEX). There needs to be greater awareness of potential cost savings across government to support this mind shift, helping leaders make informed changes.

To help with transitioning toward a cloud-friendly procurement approach, **Australia**'s Digital Transformation Agency has proposed changes to agile funding and government procurement models that help agencies make more frequent and smaller-scale expenditure decisions (footnote 34).

The Government of **Singapore**'s Commercial Cloud Infrastructure project was established to accelerate the procurement process by granting government agencies quick clearances for cloud service procurement from private sector offerings.[36]

[36] A. Tan. 2019. How AWS is Cracking the Public Sector Cloud Market. *Computer Weekly.* 10 October; and Singapore Government Developer Portal. Government Commercial Cloud. https://www.developer.tech.gov.sg/technologies/infrastructure-and-hosting/government-commercial-cloud

C. Human Resource Legacy Issues in Skills Development and Acquisition

To effectively harness cloud computing technologies, governments need to ensure that their employees are equipped with the right skills. This includes the ability to understand how cloud affects procurement and budgeting decisions, apply best practices for the migration to cloud, and implement effective cloud management and cybersecurity practices.

For an effective cloud adoption and migration, governments must ensure that both IT and non-IT personnel (e.g., finance, procurement, and legal departments) are trained on the merits of the cloud, and understand how cloud may require shifts in their existing workflows or policies.

Governments typically have older workforces who may be more comfortable with legacy computing infrastructure.

The demand for cloud computing skills is rising exponentially and organizations around the world are facing talent shortages, making recruitment a barrier for cloud adoption that is quite common in government institutions, exacerbating common human resource management challenges, which include:

- a workforce that is more comfortable with legacy computing infrastructure,
- lack of relevant skills to maintain a cloud-based computing infrastructure, and
- difficulties in hiring and retaining tech-savvy workers.

➢ Solution: Workforce Retraining

Skills gap-related challenges can be addressed through upskilling and retraining programs that equip existing employees with skills and knowledge required for cloud migration and the subsequent maintenance of the cloud environment.

When **Thailand** announced its plans to embark on a Government Data Center and Cloud Service project to create a central government cloud system, it included extensive training for 2,500 employees in the total budget of the project of B4.75 billion ($146.6 million in 2020).[37] This has been further built out into the project's certification program with three levels of certification available: Essential, Advanced, and Expert.[38]

IT and human resource departments should conduct a skills gap analysis to map the skills of the current workforce against the skills required and develop reskilling strategies that address these gaps. Cloud computing certifications and other capacity-building programs offered by cloud service providers can be tapped as reskilling opportunities. Numerous certification courses are offered by the private sector. These include:

- Amazon Web Services offers cloud computing training courses for government employees.[39]
- Google Cloud offers training in Google cloud,[40] and hosts frequent Public Sector Connect events to discuss and train government civil servants.[41]
- Microsoft launched an artificial intelligence business school for public servants in 2019.[42]

---

37 C. Theparat. 2020. Funding for State Cloud Approved. *Bangkok Post*. 6 May.
38 Thailand Government Data Center and Cloud Service. Training. https://gdcc.onde.go.th/training/
39 Amazon Web Services. Training and Certification for Government. https://gdcc.onde.go.th/training/
40 Google. Google Cloud Training. https://cloud.google.com/training
41 Google. Public Sector Connect. https://cloudonair.withgoogle.com/events/public-sector-summit?tab=community
42 J. Barnett. 2019. Microsoft Launches Online AI Course for Government Employees. *Fed Scoop*. 30 May.

- Huawei runs their Huawei Cloud Academy with free courses.[43]
- Alibaba Cloud runs e-learning courses via their online Academy.[44]

➢ **Solution: Reform of Human Resource Management**

Addressing the difficulties in hiring and retaining tech-savvy workers who may prefer to work in leading technology companies or start-ups will require a review and update of recruitment and hiring approaches, strategies and practices.

To attract technology talent, **Singapore**'s GovTech revised its human resource recruitment and development scheme to match the salaries that technology talents would otherwise command in the private sector and has begun recruiting overseas Singaporeans through recruitment drives in Silicon Valley. Recognizing that acquiring talent is pointless if high turnover depletes the ranks soon after, GovTech introduced a new scheme for public sector digital technology hires, allowing them to gain exposure across different agencies, boosting the value and job satisfaction of public sector roles.[45]

IV. RECOMMENDATIONS ON HOW GOVERNMENTS CAN EFFECTIVELY ADOPT CLOUD COMPUTING

A. Create Pro-Cloud Regulatory Conditions

A study by Gartner found that concerns about data privacy and security were two of the top barriers to cloud adoption in the public sector.[46] A government's ability and decision to maximize the benefits of cloud computing technology by using cloud services in a confident and secure manner is contingent on the laws and regulations that govern their electronic systems and data. Among these would be robust fit-for-purpose data protection and cybersecurity frameworks that ensure a good balance between protecting national security, safeguarding citizens' data, and ensuring that the development of the digital economy and its requisite data flows are not overly restricted by data regulations.

Data localization does not equate to data security.

Regulatory approaches to data protection and security have a direct impact on the way agencies use cloud. Data localization requirements, for one, reflect a perception that in order to have oversight and access to data, it must be stored within the country. In Asia, data localization measures have been proposed or enacted in the People's Republic of China; Hong Kong, China; India; Indonesia; Malaysia; Thailand; and Viet Nam—most often within broader data protection, cybersecurity, or national defense policies. Likewise, many policies make it increasingly expensive, complicated, or unfeasible to transfer data transnationally, posing a major threat to the cloud computing business model and limiting agencies' choice of cloud services.[47]

---

43 Huawei Cloud Academy. Learning Paths. https://edu.huaweicloud.com/intl/en-us/
44 Alibaba Cloud Academy. E-Learning Courses. https://edu.alibabacloud.com/elearning
45 *GovTech Singapore*. 2019. Digital Government, Smart Nation: Pursuing Singapore's Tech Imperative. 30 August.
46 R. van der Meulen. 2018. Understanding Cloud Adoption in Government. *Gartner*. 11 April.
47 Salesforce. 2019. *Japan Leads G20 Countries in Cross-Border Data Flows–New Salesforce Study Finds*. 24 June.

Enable cross-border data transfers via data accountability mechanisms.

A more practical alternative is for governments to put in place legal mechanisms for data accountability that must be complied with by businesses and governments transferring data between jurisdictions with different data protection and/or privacy regimes. Multilateral frameworks such as the Association of Southeast Asian Nation (ASEAN) Data Management Framework and the ASEAN Model Contractual Clauses can be leveraged to bridge this gap as such mechanisms help government agencies easily identify interoperable or equivalent data protection standards without having to prescribe specific requirements for each vendor or contract.[48]

The Cross-Border Privacy Rules (CBPR) system of the **Asia-Pacific Economic Cooperation (APEC)** is an accountability-based framework that provides for implementation flexibility and promotes interoperability, while ensuring that certified companies demonstrate compliance to a consistent set of standards and requirements. **Singapore**, which is a CBPR participant, recognizes CBPR-certified overseas recipients of personal data as having comparable protection to organizations legally bound by domestic privacy law.[49]

Unfortunately, despite efforts to increase its adoption, the APEC CBPR has had limited practical impact as only a limited number of companies have implemented CBPR.[50] It may therefore be useful to take a combination approach using both regional approaches like the CBPR together with international technical standards such as the ISO/IEC 27000 series governing information security.[51]

Implement a data classification framework.

Regulations play a key role in facilitating secure cloud adoption. However, privacy or security requirements that assign a stringent level of protection to all levels of public sector data may inhibit the use of general-purpose cloud-based applications (e.g., human resource management software, digital collaboration platforms) or lead to agencies choosing less optimal services because of perceived security risks.

Data classification is a tool that governments can use to assign different levels of security measures to different categories of data, based on their perceived risk impact (i.e., the criticality or sensitivity of data), to help agencies determine the appropriate level of protection required. This risk-based data classification approach will allow each type of public sector data involved in a process or service that is being considered for migration to the cloud to then be classified and handled accordingly (Table 1).

Table 1: Data Classification and Government Data

Data Classification Type	Amount of Government Data	Cloud Deployment
Low sensitivity	High	Public Cloud
Medium sensitivity	Few	Hybrid Cloud
High sensitivity	Rare	Private Cloud

[48] *Personal Data Protection Commission of Singapore*. 2021. ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows. 22 January.

[49] *Personal Data Protection Commission of Singapore*. 2020. Singapore Now Recognises APEC CBPR and PRP Certifications under PDPA. 2 June.

[50] Cross-Border Privacy Rules System. CBPR System Directory. http://cbprs.org/compliance-directory/cbpr-system/

[51] B. Lewis. 2018. ISO/IEC 27000—Key International Standard for Information Security Revised. *International Organization for Standardization*. 1 March.

Table 2 shows examples where governments have used data classification.

Table 2: Government Statements on Data Classification

Government	Public Sector Data Classification
Singapore GovTech press release on Leveraging Commercial Cloud to Accelerate Digital Transformation	Less sensitive government information and communications technology systems to be hosted on commercial cloud, while small number of very sensitive and critical systems will remain hosted within government.
United Kingdom's Guidance, Public Sector Use of Cloud (2017)	Vast majority of government information and services suitable for commercial cloud services, but a risk-based assessment of cloud use may show that there may be a small number of situations where it may not be appropriate to use cloud services for specific systems or data.
Australia Digital Transformation Agency's Secure Cloud Strategy 2018	Cloud computing use in the public sector should be based on risk assessment and matching appropriate security controls, rather than checking off compliance requirements. The public sector should also consider moving high and low value information into different environments to increase flexibility and focus resources.
Philippines Department of Information and Communications Technology Amendments to Department Circular 2017–002, Re: Prescribing the Philippine Government's Cloud First Policy	Defines four levels of data classification for the public sector: • Highly sensitive government data • Above-sensitive government data • Sensitive government data • Non-sensitive government data
Philippines Department of Information and Communications Technology Amendments to Department Circular 2017–002, Re: Prescribing the Philippine Government's Cloud First Policy	Defines four levels of data classification for the public sector: • Highly sensitive government data • Above-sensitive government data • Sensitive government data • Non-sensitive government data

Sources: Australian Government Digital Transformation Agency. 2017. *Secure Cloud Strategy*; Government of the United Kingdom. 2017. *Guidance: Public Sector Use of the Public Cloud*. 16 January; GovTech Singapore. n.d. *Leveraging Commercial Cloud to Accelerate Digital Transformation*. Media Factsheet; and Philippine Department Information and Communications Technology. 2020. *Amendments to Department Circular No. 2017–002, Re: Prescribing the Philippine Government's Cloud First Policy*.

There may be a risk of over-classifying content by ministry officials, where data is categorized to be a higher sensitivity level than required. Ongoing training and awareness-raising in the government on how to implement and maintain a risk-based data classification framework will be useful to mitigate against over-classification of data.

Address central and local government policy conflicts.

To create interoperable cloud systems, conflicting regulations at the central and local government levels should also be reconciled.

In **Japan**, the central government is governed by the Act on the Protection of Personal Information Held by Administrative Organs, which comes in addition to the national privacy framework, Act on the Protection of Personal Information. Local governments, on the other hand, are required to comply with the Personal Information Protection Ordinance. The result has been an overall lack of optimization as e-government initiatives are carried out independently by various local governments. This has led organizations to apply different standards, resulting in incompatible data formats and IT systems,[52]

[52] *Keidanren (Japan Business Federation)*. 2017. Establishing e-Government with the Aim of Realizing Society 5.0. 14 February

and making it difficult for agencies to reach a common approach to cloud deployment. The planned formation of a new government digital agency in September 2021 would be one step toward addressing this fragmentation in local and central government policy.[53]

In addition to establishing expectations for data privacy and security, regulation can also act as a driving force toward cloud adoption.

In the **Philippines**, the Electronic Business Permits and Licensing System has been made compulsory by the Anti-Red Tape Authority through Republic Act 11032,[54] which requires all local government units to automate their Business Permit Systems by 2021.[55] The Department of Information and Communications Technologies schedules training sessions with IT staff in each local government unit before the system is launched and implemented.

Governments should:

- Assess key bottlenecks in terms of data management, data classification, and interoperability between government service platforms.
- Develop (and update) cloud-relevant data privacy regulation, and raise awareness among relevant staff of its importance.
- Develop (and update) cloud-relevant cybersecurity regulations, and improve staff awareness (including basic and advanced cyber training), intelligence capabilities, establish or bolster computer emergency response teams and enforcement.
- Leverage internationally recognized standards and best practices, and support regional initiatives that enable data portability and establish consistency across regulatory regimes.

B. Create a Robust Cloud Strategy and Adoption Plan

The establishment of a national cloud first or cloud-by-default policy could signal a government's receptiveness toward cloud computing. This should be followed up with a clear implementation plan or strategy, which could then be iterated to suit the requirements of the country and incorporate the learnings from earlier implementations.

In the **US**, the 2010 federal "Cloud First" policy was replaced by a "Cloud Smart" strategy, which addressed the adoption issues faced by agencies under the previous policy.[56] The former "Cloud First" policy deployed cloud computing for the public sector through any means possible (an indiscriminate policy), while the new "Cloud Smart" policy provides more guidance and suggests giving priority to cloud thanks to its advantages, while allowing other options to be adopted.[57]

Similarly, **Australia**'s Digital Transformation Agency in 2018 launched the Secure Cloud Strategy, a new iteration of the 2014 Cloud Computing ("Cloud First") Policy, to assist agencies in developing cloud strategies that cater to their individual needs.[58] The original policy was developed by the Department of Finance and focused on a "Cloud First" policy from a procurement standpoint. When the Digital

---

53 The Jiji Press. 2016. Japan Plans to Set Up Digital Agency in Sept. 2021. *Nippon*. 16 November.

54 Section 26 of Republic Act 11032 mandates that the Department of Information and Communications, in coordination with other concerned agencies, must automate business-related transactions by developing the necessary software and technology-neutral platforms and secure infrastructure that is web-based and accessible to the public.

55 R. Canivel. 2020. Online Processing of Building, Occupancy Permits Pushed. *Inquirer.Net*. 17 September.

56 Office of Management and Budget of the United States Government–Office of the Federal Chief Information Officer. Federal Cloud Computing Strategy. https://cloud.cio.gov/#:~:text=The%202019%20Federal%20Cloud%20Computing,safe%20and%20secure%20cloud%20infrastructure

57 M. Hensch. 2019. *Moving from Cloud First to Cloud Smart*. 19 March.

58 Digital Transformation Agency of the Australian Government. Secure Cloud Strategy. http://www.dta.gov.au/what-we-do/policies-and-programs/secure-cloud

Transformation Agency took over the policy development for government cloud, it refocused the policy onto a competency-based approach that, similar to the US policy adjustment, focused the government on its ability to use cloud in a way that "maintains security, integrity, and availability for critical government systems across all cloud deployment and service models" (footnote 63).

Other economies with cloud strategies include the United Kingdom's Government Cloud First policy,[59] the Singapore Government Cloud Strategy,[60] and the Philippines' Government Cloud First Policy.[61]

Prioritize and define the scope of government cloud migration.

When first adopting cloud, government agencies should consider a prioritization of use cases that are likely to demonstrate the highest impact (e.g., citizen-facing services, back-office systems, interoperability solutions) and build internal capacity. Most government agencies conduct a thorough risk assessment to select use cases that are both high-impact and non-critical as initial pilots and proofs of concepts.

A well-defined scoping of cloud migration or application development projects is key to success (Box 2). When developing new citizen services, there is often a desire to address all citizen needs within a single project. Yet a lack of resources and changing definitions for cloud migration, including adjustments in technical requirements, project scope, deployment timeframes, key purpose, deliverables, and a lack of appropriate and skilled management support, can add significantly to the challenge.[62]

Box 2: Steps for Defining the Scope of Cloud Migration

1. Define the project terms of reference.
2. Involve the right people in defining the project scope.
3. Accurately define processes.
4. Define process boundaries explicitly.
5. Outline high-level interfaces between processes (interoperability aspects).
6. Conduct a "health check" on the process interfaces.
7. Review project scope to check whether the project is too large to manage. By reducing the project scope, governments can minimize development and administrative costs, as well as achieve time savings.

Sources: Amazon Web Services. How to migrate. https://aws.amazon.com/cloud-migration/how-to-migrate/; Google Cloud. Migration to Google Cloud: Getting Started. https://cloud.google.com/solutions/migration-to-gcp-getting-started; Islam, Shareeful et al. 2014. *A Decision Framework Model for Migration into Cloud: Business, Application, Security and Privacy Perspectives*; Microsoft Azure. How to migrate. https://azure.microsoft.com/en-us/migration/migration-journey/; and National Institute of Standards and Technology. 2011. *US Government Cloud Computing Technology Roadmap Volume II.*

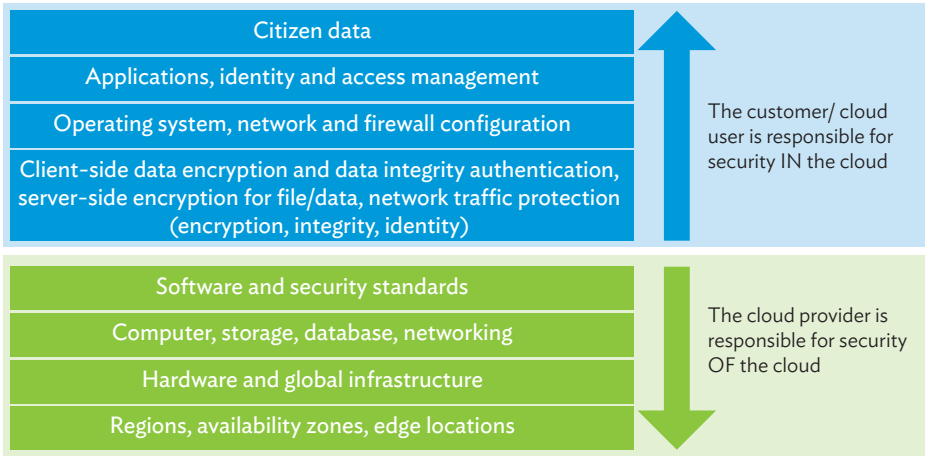
Background reading: Gholami, Mahdi Fahmideh. 2016. Cloud Migration Process–A Survey, Evaluation Framework, and Open Challenges. *The Journal of Systems and Software.* 120: 31–69; The Modern Analyst. Process Mapping 101: A Guide to Getting Started. https://www.modernanalyst.com/Resources/Articles/tabid/115/ID/892/Process-Mapping-101-A-Guide-to-Getting-Started.aspx; Pahl, Claus et al. n.d. *A Comparison of On-Premise to Cloud Migration Approaches.*

[59] Government of the United Kingdom. 2017. *Government Cloud First Policy*.
[60] Infocomm Development Authority of Singapore. *Cloud Computing for Singapore Government*. Fact Sheet.
[61] Government of the Philippines, Department Information and Communications Technology. 2020. *Amendments to Department Circular No. 2017–002, Re: Prescribing the Philippine Government's Cloud First Policy*.
[62] Amazon Web Services. 2016. *Stop Wasting Money, Move Faster, and Innovate.*

Given the flexibility of cloud computing environments, it is possible to first focus on a single issue and to develop an application that addresses that specific need; and to then iterate upon it with updates and adaptations, while the first application is being tested or deployed. This can minimize the impact of challenges during application development, allowing real-world piloting and iterative improvements.

If a government agency intends to deploy a hybrid or public cloud, an important data governance concept to consider is the shared responsibility model (Figure 6). Defining the terms of reference would need to include discussing which entity is responsible for which data. When moving to cloud, some government agencies (the data controller) assume that the cloud service provider (the data processor) is responsible for the security of the data, which is only partially true. A discussion of the cloud service provider's responsibilities at various data levels would be prudent to include in scoping government data being moved to the cloud.

Figure 6: Shared Responsibility Model



Source: Derived from Amazon Web Services. Shared Responsibility Model. https://aws.amazon.com/compliance/shared-responsibility-model/

Consider small pilot projects to gain migration experience.

Another key consideration is the ease of transitioning to a cloud computing environment. It may be useful to pilot the cloud migration for services that are simpler to migrate, and where a quick success encourages and emboldens the agency to tackle larger cloud migrations with increasing confidence, familiarity, and skills.

Currently, a common approach is to wait to move to the cloud until legacy systems reach their end of life, delaying cloud adoption. If the expressed goal is to transition to cloud, defining an end goal and a targeted completion date can provide agencies with an impetus to move forward and indicators to gauge the success of their cloud strategy.

Establish a new government unit to coordinate cloud transitions for the public sector.

To better support agencies in their cloud adoption journey, governments can consider creating a central or inter-agency Cloud Center of Excellence (CCOE) that assists cloud adoption and oversees practices. The CCOE can unify government IT departments across agency silos to share knowledge, resources (e.g., common code and services) and best practices (e.g., in procurement and migration), as well as support the development of robust cloud strategies.

One survey found that 96% of public sector respondents believed that they would benefit from a CCOE through reduced security risks and costs, and better ability to be innovative and agile.[63] Having a central entity to manage requirements and use can be an important catalyst for cloud adoption.

Build on existing solutions created by others.

To speed up the cloud implementation process, governments can encourage agencies to build applications using common resources or tried-and-tested open solutions.

The **Singapore** government's Technology Stack is a centralized platform that allows government agencies to build and test new digital applications with support from the national ICT regulator, the Infocomm Media Development Authority. This helps maintain consistency and quality of applications and allows agencies to speed up their delivery of cloud-based services by leveraging reusable common services, such as the National Digital Identity for authentication.[64]

Establish a strong cloud foundation for innovation narrative for the public sector.

Finally, governments should ensure that cloud enablement is a key consideration when promoting emerging digital technologies through national-level strategies. Cloud enablement strategies involve going beyond a simple cloud-first policy, and work to develop and implement approaches that help enable governments to easily and simply implement the policy.

Cloud enablement is important because it takes broad cloud support policies, such as cloud-first policies, and operationalizes them into actionable steps for decision makers to implement. This helps to reinforce the importance of cloud as a foundational technology and encourages the implementation of cloud strategies across agencies as it relates to issues of national significance.

For example, as part of its digital transformation initiative, the Government of **Australia** has recognized the cloud as being a foundational platform for leveraging emerging technologies such as artificial intelligence, blockchain, and quantum computing, and intends to provide all agencies with access to cloud systems.[65] This has resulted in a reconfiguration of the government's digital marketplace for cloud services, which has now made available cloud services and vendors as pre-approved panel selections from which government agencies may procure advanced cloud supported services.[66]

Another approach could be to expand public–private partnerships to leverage the cloud. For example, **India**'s Ministry of Electronics and Information Technology has partnered with Amazon Web Service's Quantum Computing Applications Lab to support India's aspirations for technology innovation. It leverages quantum computing as a service to India's government ministries and departments, and also springboards to serve the broader Indian research and development community.[67] The US government has also launched a large public–private partnership with Amazon Web Services, IBM, Google Cloud Platform, Microsoft, and other cloud computing companies to form the COVID-19 High Performance Computing Consortium, where cloud computing, high-performance computers, and government data,

---

63 J. Sorenson and M. Hong. 2019. How a Center of Excellence Can Fuel Cloud Success. *Washington Technology*. 2 April.

64 *GovTech Singapore*. 2020. Doubling Down on Cloud to Deliver Better Government Services. 24 June.

65 J. Mariani et al. 2019. Cloud as Innovation Driver: The Foundation for Employing Emerging Technologies in Government. *Deloitte Insights*. 24 June.

66 Digital Marketplace of the Australian Government. 2020. *AGD-ICT-RFQ-138—Artificial Intelligence / Machine Learning Services*. 4 August.

67 S. Dhapola. 2021. MeITY and AWS announced Quantum Computing Applications Lab in India. *The Indian Express*. 19 January.

will work together to accelerate understanding of the virus and the development of treatments and vaccines.[68]

When embarking on cloud adoption, governments should:

- Consider adopting a cloud-first or cloud-by-default approach as a whole-of-government approach.
- Clearly define and manage the scope and timeline of projects.
- Retrain IT professionals and give them clear career paths, focusing on new skills.
- Ensure that procurement vehicles are suitable for cloud computing.
- Consider the creation of internal support teams that provide advisory services and support to agencies, integrating or building new cloud services. This may include a coordination function (e.g., CCOE) and lab structures to prototype and trial new solutions.
- Ensure that strategies and road maps for advanced technologies (such as artificial intelligence) acknowledge the foundational role of cloud and consider the linkages with the cloud strategy.

V. CONCLUSION

Governments around the world are digitally transforming the way they deliver citizen services through cloud computing. Rapid changes in technology have created opportunities for governments to take advantage of the benefits of cloud computing to reduce the costs of upgrading legacy technologies, develop new and agile mechanisms for e-government, allow human resource skill set upgrading, and improve public sector resilience and recovery capabilities in times of crisis.

However, there are still barriers to widespread public sector adoption of cloud computing, such as the need for government policy makers to better understand cloud computing characteristics, and for more training to implement data protection and security for government cloud.

Government-wide policy adjustments could also be made, such as reworked purchasing mechanisms to enable an easier cloud computing selection and procurement, and the reform of human resource management to ensure that a steady stream of trained technology staff are hired to support the use of cloud technologies by the government.

Governments should therefore strive to create enabling regulatory conditions that support public sector use of cloud computing. It is best that these regulations are iterated on a regular basis by a central authority, to address a possible fragmentation of policy approaches. This includes coordinating regionally to achieve greater consistency of accountability requirements and the adoption of international technical standards governing information security, which would enable cross-border information sharing and promote interoperability.

Governments should also work to ensure a clear and robust cloud strategy, such as a cloud migration and/or implementation approach, underpinned with an overarching policy such as a cloud-first strategy. Other supporting cloud enablement mechanisms should also be developed, such as the development of a suitable government unit or CCOE to support cloud technology adoption, and a cloud procurement marketplace to allow fast and safe assessment and purchase of cloud services for public sector deployment.

[68] J. Panettieri. 2020. AWS, IBM, Google, Microsoft, join COVID-19 HPC Consortium. *Channele2e.* 22 March.

REFERENCES

Asian Development Bank (ADB). 2019. ADB-Supported Irrigation Project to Improve Kazakhstan's Agricultural Productivity. News release. 11 September.

Alibaba Cloud. Elastic Compute Services (Subscription) Price Calculator. https://www.alibabacloud.com/pricing-calculator#/add/acm-195b9957-d5b9-41ae-9ae2-b0903fd802fd/vm_intl/vm_intl

Alibaba Cloud Academy. E-Learning Courses. https://edu.alibabacloud.com/elearning

Amazon Web Services. Amazon Web Services Pricing Calculator. https://calculator.aws/#/createCalculator/EC2

———. 2016. *Bureau of Customs of the Philippines Case Study*.

———. 2016. *Land Transport Authority of Singapore Case Study*.

———. 2016. *Stop Wasting Money, Move Faster, and Innovate*

———. How to Migrate. https://aws.amazon.com/cloud-migration/how-to-migrate/

———. Shared Responsibility Model. https://aws.amazon.com/compliance/shared-responsibility-model/

———. Training and Certification for Government. https://aws.amazon.com/training/government/

Australian Cybersecurity Centre. 2020. *Cloud Services*.

Australian Government Digital Transformation Agency. 2017. *Secure Cloud Strategy*.

Azerbaijan Council. 2019. *Digital Bridge between Europe and Asia, 2019–2022*.

Barnett, J. 2019. Microsoft Launches Online AI Course for Government Employees. Fed Scoop. 30 May.

Canivel, R. 2020. Online Processing of Building, Occupancy Permits Pushed. Inquirer.Net. 17 September.

Cross-Border Privacy Rules System. CBPR System Directory. http://cbprs.org/compliance-directory/cbpr-system/

Deloitte. 2019. Harnessing Public Cloud Opportunities in the Government Sector. Access Economics. 22 March.

Dhapola. S. 2021. MeITY and AWS announced Quantum Computing Applications Lab in India. The Indian Express. 19 January.

Dharmaraj, S. 2020. Vietnam Aims to Become a Digital Society by 2030. Open Gov Asia. 8 June.

Digital Marketplace of the Australian Government. 2020. *AGD-ICT-RFQ-138—Artificial Intelligence / Machine Learning Services*. 4 August.

Digital Transformation Agency of the Australian Government. Secure Cloud Strategy. http://www.dta.gov.au/what-we-do/policies-and-programs/secure-cloud

Eggers, W. et al. 2019. The Future of Work in Government: Navigating a Shifting Talent Landscape. *Deloitte*. 28 February.

Gholami, Mahdi Fahmideh. 2016. Cloud Migration Process–A Survey, Evaluation Framework, and Open Challenges. *The Journal of Systems and Software.*

Google. Google Cloud Training. https://cloud.google.com/training

———. Public Sector Connect. https://cloudonair.withgoogle.com/events/public-sector-summit?tab=community

———. Google Cloud Pricing Calculator. https://cloud.google.com/products/calculator

———. Migration to Google Cloud: Getting Started. https://cloud.google.com/solutions/migration-to-gcp-getting-started

Government of the Philippines, Department of Information and Communications Technology. 2020. *Amendments to Department Circular No. 2017–002, Re: Prescribing the Philippine Government's Cloud First Policy*.

Government of the United Kingdom. 2017. *Guidance: Public Sector Use of the Public Cloud*. 16 January.

———. 2017. *Government Cloud First Policy.*

GovTech Singapore. 2020. Doubling Down on Cloud to Deliver Better Government Services. 24 June.

———. 2019. Digital Government, Smart Nation: Pursuing Singapore's Tech Imperative. 30 August.

———. 2018. Getting to Know NECTAR and APEX. 24 July.

———. n.d. *Leveraging Commercial Cloud to Accelerate Digital Transformation*. Media Factsheet.

———. n.d. *Singapore Government Tech Stack*.

Harms, R. and Yarmartino, M. 2010. *The Economics of the Cloud*.

Hensch, M. 2019. *Moving From Cloud First to Cloud Smart*.

Ho, G. 2020. Singaporeans Can Soon View their Bank Accounts and Investments on a Single Platform. The Straits Times. 1 December.

Huawei Cloud. Elastic Cloud Service Price Calculator. https://www.huaweicloud.com/intl/en-us/pricing/#/ecs

Huawei Cloud Academy. Learning Paths. https://edu.huaweicloud.com/intl/en-us/

Infocomm Development Authority of Singapore. *Cloud Computing for Singapore Government*. Fact Sheet.

———. 2021. *Compliance and Certification*. 7 January.

———. 2020. *Cloud Computing and Services*. 10 December.

———. 2013. *New Multi-Tier Cloud Security Standard in Singapore*. 13 November.

Islam, Shareeful et al. 2014. *A Decision Framework Model for Migration into Cloud: Business, Application, Security and Privacy Perspectives*.

ISO. 2018. *ISO/IEC 27000: Key International Standard for Information Security Revised*.

ISO. 2015. *ISO/IEC 27017: Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

Kazimbeyli, Y. 2019. Azerbaijan's Largest Airport Pioneers Cloud Computing. *Caspian News*. 5 July.

Keidanren (Japan Business Federation). 2017. Establishing e-Government with the Aim of Realizing Society 5.0. 14 February.

Kivity, S. 2020. 3 Hard-Won Lessons from a Decade of Negative Cleantech Returns. *World Economic Forum*. 13 March.

Lewis, B. 2018. ISO/IEC 27000—Key International Standard for Information Security Revised. *International Organization for Standardization*. 1 March.

Mariani, J. et al. 2019. Cloud as Innovation Driver: The Foundation for Employing Emerging Technologies in Government. *Deloitte Insights*. 24 June.

Mastercard. 2020. FinTech in 2020: Five Global Trends to Watch (CB Insights in Partnership with Mastercard Start Path). January.

Mell, P. and Grance, T. 2011. *The National Institute of Standards and Technology Definition of Cloud Computing: Recommendations*.

Microsoft. 2020. City Government of Osaka. 16 September.

———. 2020. Multi-Tier Cloud Security Standard for Singapore. 1 January.

———. 2020. Philippine Government Automates Business Permits and Licensing System. 30 April.

———. 2019. Thailand's AI-Powered Healthcare System Curbs Government Costs, Helps Save Lives. 26 April.

Microsoft Azure. How to Migrate. https://azure.microsoft.com/en-us/migration/migration-journey/

———. Pricing Calculator. https://azure.microsoft.com/en-us/pricing/calculator/

National Institute of Standards and Technology. 2011. *US Government Cloud Computing Technology Roadmap Volume II*.

Office of Management and Budget of the United States Government–Office of the Federal Chief Information Officer. Federal Cloud Computing Strategy. https://cloud.cio.gov/

Pahl, Claus et al. n.d. *A Comparison of On-Premise to Cloud Migration Approaches*.

Panettieri. J. 2020. AWS, IBM, Google, Microsoft, join COVID-19 HPC Consortium. *Channele2e*. 22 March.

Personal Data Protection Commission of Singapore. 2021. ASEAN Data Management Framework and Model Contractual Clauses on Cross Border Data Flows. 22 January.

———. 2020. Singapore Now Recognises APEC CBPR and PRP Certifications under PDPA. 2 June.

Robinson, B. 2020. Legacy Systems: Too Old to Die? *GCN: The Technology that Drives Government IT*. 16 April.

Salesforce. 2019. Japan Leads G20 Countries in Cross-Border Data Flows–New Salesforce Study Finds. 24 June.

———. n.d. *Cloud Adoption in Government: Salesforce Drives DCSI Service Innovation to Improve the Lives of People with Disabilities.*

Schneider Electric. Data Center Capital Cost Calculator. https://www.se.com/ww/en/work/solutions/system/s1/data-center-and-network-systems/trade-off-tools/data-center-capital-cost-calculator/

Shin, H. et al. 2020. How South Korea Turned an Urban Planning System into a Virus Tracking Database. *Reuters*. 22 May.

Singapore Government Developer Portal. Government Commercial Cloud. https://www.developer.tech.gov.sg/technologies/infrastructure-and-hosting/government-commercial-cloud

Smart Energy International. 2020. Tajikistan's Digital Transformation Wins Korea and World Bank Support. 6 February.

Sorenson, J. and Hong, M. 2019. How a Center of Excellence Can Fuel Cloud Success. *Washington Technology*. 2 April.

Tan, A. 2019. How AWS is Cracking the Public Sector Cloud Market. *Computer Weekly*. 10 October.

Thailand Government Data Center and Cloud Service. Training. https://gdcc.onde.go.th/training/

The Jiji Press. 2016. Japan Plans to Set Up Digital Agency in Sept. 2021. *Nippon*. 16 November.

The Modern Analyst. Process Mapping 101: A Guide to Getting Started. https://www.modernanalyst.com/Resources/Articles/tabid/115/ID/892/Process-Mapping-101-A-Guide-to-Getting-Started.aspx

Tham, I. 2020. GovTech Launched to Lead Digital Transformation in Public Sector. *The Straits Times*. 27 July.

Theparat, C. 2020. Funding for State Cloud Approved. *Bangkok Post*. 6 May.

United Nations. 2020. *United Nations e-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development.*

Van der Meulen, R. 2018. Understanding Cloud Adoption in Government. *Gartner*. 11 April.

Viet Nam Net Global. 2019. Young Students Design Made-in-Da Nang Trash Collector. 17 June.

Western Australian Government–Office of Digital Government. 2019. Landgate–Cloud Transition Case Study. 1 February.

Wray, S. (ed). 2020. India Pledges Five More Smart Cities. *Smart Cities World*. 3 February.

Xu, Q. 2020. Planning for Lockdown and How to Emerge Out of It. *University World News*. 25 April.

24.KG. 2018. Kyrgyzstan Develops Concept of Digital Transformation. 14 December.

Cloud Computing as a Key Enabler for Digital Government across Asia and the Pacific

Governments are responding to rapid change and growing demands by citizens and businesses by accelerating the digitalization of public services. They are updating their e-government capabilities, adding new digital tools and services, augmenting their data analytics capabilities, and putting in place digital economy development plans. Many of these changes are enabled by cloud computing technologies that have become commonplace in the digitally connected world. The rapidly scalable computing resources that cloud computing delivers via the internet bring cost benefits, improve agility, ensure resilience, and provide access to the latest solutions that digital technology can offer.

About the Asian Development Bank

ADB is committed to achieving a prosperous, inclusive, resilient, and sustainable Asia and the Pacific, while sustaining its efforts to eradicate extreme poverty. Established in 1966, it is owned by 68 members —49 from the region. Its main instruments for helping its developing member countries are policy dialogue, loans, equity investments, guarantees, grants, and technical assistance.

ADB

ASIAN DEVELOPMENT BANK
6 ADB Avenue, Mandaluyong City
1550 Metro Manila, Philippines
www.adb.org