



# Role of Governments in Promoting Cloud Adoption

# 6

## ABSTRACT

This chapter explores the role of governments in shaping cloud and data infrastructure markets using the policies, initiatives, and strategies that they can implement.

## MAIN MESSAGES

- Governments play a key role in steering the development of cloud and data infrastructure markets. Robust national digital transformation strategies and government use of cloud technologies can promote economywide adoption.
- Cloud-first or cloud-smart policies are becoming increasingly common in middle-income economies and ubiquitous in high-income economies. Hybrid and multicloud deployments for government use are also rising.
- Data quality and data classification frameworks are critical to cloud migration efforts.
- Small and medium enterprises and start-ups play pivotal roles in numerous economies. Consequently, many countries are actively pursuing their digitalization<sup>1</sup> and the enhanced adoption of new technologies—including cloud services, data analytics, and artificial intelligence—to support and bolster these vital sectors. Public support schemes for business digitalization and start-up acceleration initiatives can enhance the technological readiness of local private sector actors, enabling their participation in the cloud ecosystem.
- The cloud-ready digital skills gap presents a pervasive challenge, affecting countries worldwide and spanning both private and public sectors. Notably, the public sector in low- and middle-income countries is more vulnerable. Recognizing its importance, governments are increasingly taking a proactive role in addressing the skills gap.

## NATIONAL DIGITAL TRANSFORMATION STRATEGIES

Governments are adopting national digital strategies to shape digital transformation in their countries. These strategies outline a clear long-term vision for digital transformation, clear priorities and objectives, measurable targets supported by sufficient financial and human resources, and a robust monitoring and evaluation mechanism. Comprehensive digital transformation strategies span multiple sectors and involve collaboration between public and private sectors to make progress on national development priorities. Effective implementation of these strategies, which also provide governments with a decision-making framework to guide resource allocation to desired outcomes, requires good governance and political stability. Such strategies, when effectively implemented, can signal stability and interest to investors. The top countries in the Global Cloud Ecosystem Index for 2022<sup>2</sup> have all adopted holistic approaches to their national digitalization efforts, with a strong emphasis on developing digital infrastructure and skills, and a commitment to regulatory clarity.

The form, content, and governance of national digital strategies vary significantly across countries. Only half of all countries have official national digital transformation strategies covering multiple economic sectors.<sup>3</sup> Awareness is increasing, however: by 2023, 30 percent of countries had made progress in establishing an advanced national digital policy and legal and governance frameworks. Comprehensive national digital transformation strategies should embrace cloud technologies while aligning with other essential objectives, such as broadband expansion, energy infrastructure improvements, fostering a skilled labor force, and seeking to create an enabling environment with a favorable business environment and effective regulatory framework.

## CLOUD-FIRST AND CLOUD-SMART NATIONAL STRATEGIES

Governments can be important catalysts for market expansion by adopting cloud technologies. Their use of cloud services sends a strong signal of confidence in technology in nascent markets. It also fuels demand because governments—especially in countries with a large public sector—are among the biggest users of cloud services.

*Cloud-first* policies prioritize the use of cloud computing technologies for delivering information technology services and conducting digital operations, thereby promoting a shift away from traditional on-premises infrastructure. These policies establish a strategic direction in favor of cloud services but do not necessitate migration of all systems to the cloud. Governments ultimately base their cloud migration decisions on context, and they consider security, compliance, and cost.

Most high-income countries have adopted cloud-first policies, and a growing number of middle-income countries have followed suit (box 6.1). Although some regional approaches exist, they are not common. The European Commission adopted the European Cloud

### **BOX 6.1** Examples of early adopters of cloud-first strategies in high- and middle-income countries

One of the early adopters of the cloud, the US federal government in 2010 introduced a cloud-first policy as part of the Federal Cloud Computing Strategy (Rubens 2011). This policy mandated that federal agencies prioritize cloud-based solutions when considering new information technology deployments. The government subsequently introduced technical and security standards, such as the Federal Risk and Authorization Management Program. Widespread adoption of cloud technologies by the US government has contributed to the development of a dynamic and competitive cloud market.

The United Kingdom, another early adopter, launched its whole-of-government cloud-first policy in 2013. The policy allowed each administrative branch and each member to define its own approach and timeline for migrating to the cloud. Consequently, the Welsh government implemented its four-year “Future ICT” project and moved government systems and services to the cloud between 2016 and 2019 (United Kingdom, Government Digital Service 2020). In 2020, the Scottish government implemented its own cloud-first policy for the Scottish public sector (Say 2020). The UK Cloud First policy was reevaluated in 2019 and continues to be important to the United Kingdom (United Kingdom, Central Digital and Data Office 2021).

Among low- and middle-income economies, Moldova was an early adopter of a cloud-first strategy. Its Strategic Program for Government e-Transformation, established in 2011, stipulated the need for a cloud-first policy. The strategy, adopted in 2012 and updated in 2014, established that ministries, the state chancellery, other central administrative authorities, and public entities will use the shared government technological platform, MCloud. The strategy does not allow government or public entities to have their own new centralized server and storage equipment (hardware) infrastructures, including the licensing of the components (software) of the newly created infrastructures.

Brazil’s federal government also has a cloud-first strategy and has promoted joint contracts since 2018 to facilitate the acquisition, use, and management of the cloud for the government. This strategy aims to facilitate the exchange of experiences, mutual learning, and cost savings. Argentina aims to move 80 percent of the national government’s information technology infrastructure and services to the cloud by 2027 to better leverage data for its digital transformation.

Computing Strategy in 2012, followed by the Digital Single Market Strategy in 2015 and the European Cloud Initiative in 2016 (European Commission 2019). The most recent EU Digital Strategy, referred to as the Digital Decade, lays out at least two specific objectives directly tied to cloud computing: the deployment of environmentally friendly and highly secure edge nodes, and the promotion of European businesses' engagement in cloud computing services, big data, and artificial intelligence (European Commission 2021). Cloud computing is expected to unlock 55 percent of the total economic value created by this strategy (Public First 2022). Each EU Member State aligns its national strategy with common EU objectives, resulting in a regional expansion of the cloud. In the East Asia and Pacific region, the Asia-Pacific Economic Cooperation forum is engaged in raising awareness and providing recommendations and best practices that member economies can use to establish the groundwork for their own cloud adoption and cloud policy frameworks.

Whereas cloud-first policies encourage government agencies to prioritize cloud computing solutions, *cloud-smart* policies recommend using cloud technologies strategically by taking a broader set of considerations into account. This approach encourages government agencies to assess their information technology needs and choose the most appropriate solutions, rather than migrating all applications to the cloud. A cloud-smart approach determines when and where cloud-first strategies may work best. Besides cloud-first and cloud-smart approaches, some countries are introducing guidelines to encourage adoption of cloud technologies in the public sector. Denmark has published a "Guide on the Use of Cloud Services" to support organizations through various stages of transitioning to the cloud.<sup>4</sup>

Importantly, an appropriate cloud and data infrastructure, along with a pertinent regulatory and legal framework, is crucial for the successful execution of cloud-first and cloud-smart policies. The potential financial implications and necessary investment requirements need to be assessed. For example, Argentina's digital transformation journey and efforts to implement its cloud-first policy are accompanied by the strengthening of its local cloud and data infrastructure (box 6.2).

Best-in-class cloud-first policies and guidelines also include detailed cloud services procurement frameworks that follow a standardized and transparent approach while recognizing some unique features of cloud procurement compared with traditional on-premises information and communication technology procurement models. Because procuring cloud services involves some important differences from procuring on-premises information and communication technology solutions (for example, moving from a capital expenditure model to an operating expenditure model), successful cloud policies provide clarity on how cloud procurement can occur (box 6.3 presents the example of the Philippines).

**BOX 6.2 Strengthening the local cloud and data infrastructure in Argentina**

Argentina aims to boost data use for its digital transformation through a cloud-first policy,<sup>a</sup> targeting a migration of 80 percent of the national government to cloud-based systems by 2027. Despite progress in digitizing core government operations, including moving operations to the cloud, limited data infrastructure hampers scaling these initiatives.

The 23 provinces, the Autonomous City of Buenos Aires, and the more than 2,000 municipalities in the country have a diverse and less developed set of digital government services for citizens and businesses compared with the national government. For instance, less than 15 percent of national agencies use cloud resources (Schijman and others 2020) despite efforts to improve public e-services.<sup>b</sup> Online platforms, combined with electronic authentication, have improved citizens' and businesses' access to digital government services, but their use remains limited because many provincial and municipal services have yet to join these online tools. The low availability of e-services may depend on—among other factors—the limited uptake of cloud services. Leveraging cloud technology ensures business continuity and broader accessibility to digital services, enhancing resilience against disasters, including those caused by climate events. Argentina, along with Brazil and Mexico, constitutes a significant market for public cloud in Latin America and the Caribbean, displaying substantial growth potential (Edward 2024).

To capitalize on this potential, the country is working to strengthen its local cloud and data infrastructure, expand its reach, and improve access to connectivity. There are 16 data centers in Argentina owned by various players, from telecom operators to infrastructure providers (TeleGeography 2021). The government provides shared infrastructure services to government agencies through the Argentine Company for Satellite Solutions (Empresa Argentina de Soluciones Satelitales Sociedad Autónoma [ARSAT]), which owns a medium data center. As data use and digital government services expand, ARSAT needs to expand its capacity to meet increased demand and provide new and more secure cloud computing, hosting, and housing services. ARSAT plans to build additional geographically dispersed data centers linked to the current ARSAT data center in Benavidez (Buenos Aires). The decentralization of the country's data infrastructure is expected to enhance resiliency and safety, preventing data losses in cases of external shocks, such as climate events, and therefore increasing adaptation to climate change. These data centers will adhere to international cybersecurity, climate resilience, and energy efficiency standards, ensuring open access and technological neutrality.

*(Continued)*

### **BOX 6.2 Strengthening the local cloud and data infrastructure in Argentina (Continued)**

Furthermore, the government is investing in broadband infrastructure to reach underserved localities lacking digital infrastructure. Additionally, efforts are under way to modernize the legal and regulatory frameworks concerning data protection, cybersecurity, and other areas crucial for supporting digital transformation.

*Source:* World Bank, “Strengthening Data Infrastructure to Close the Digital Gap in Argentina Project,” <https://projects.worldbank.org/en/projects-operations/project-detail/P178609>.

a. Government of Argentina, “Camino recorrido para la adopción de Nube en Gobierno,” <https://www.argentina.gob.ar/onti/camino-recorrido-para-la-adopcion-de-nube-en-gobierno>.

b. The Secretariat of Public Innovation (Secretaría de Innovación Pública) of the Chief of the Cabinet of Ministers Office (Jefatura de Gabinete de Ministros) in the national government launched a program in 2016 that supports gradual implementation of shared e-services for remote municipalities using centrally supported cloud services. This program allows municipalities to use high-quality applications at a very low cost. The national government has also provided subnational governments with administrative applications. The e-filing system has been deployed in eight provinces and the e-procurement system in four provinces, contributing to improving governance.

### **BOX 6.3 Procurement hurdles in the Philippines**

In the Philippines, the procurement process was highlighted as one of the hurdles in moving to the cloud. The country adopted a progressive Cloud First Policy in 2020—one of the first developing countries to do so. However, implementation of this policy has faced challenges. First, data classification is still based on the outdated 1964 Memorandum Circular. Second, procurement is hampered because the Department of Information and Communications Technology has yet to release a registration process for cloud service providers. Consequently, agencies must undergo the traditional budget and procurement process (in other words, public bidding) under the annual General Appropriations Act and the Government Procurement Reform Act.

Because of the lead time required for the national budget, using the traditional procurement process effectively means that agencies may need to plan at least two years in advance if they want to procure cloud services. Cloud services are still classified as a capital expenditure in the same way as traditional information technology hardware and infrastructure, rather than as a utility or operating expense.

Agencies must also take the additional step of having these procured cloud services classified as part of GovCloud. The Philippine Statistics Authority successfully completed this step for the rollout of the new national identification system that launched mass registration in 2020. Knowledge of the ad hoc GovCloud classification process does not appear widespread among other government agencies; meanwhile, the government is working on improvements, such as through harmonization of cloud procurement and medium-term planning related to information and communication technology.

The World Bank publication “Institutional and Procurement Practice Note on Cloud Computing: Cloud Assessment Framework and Evaluation Methodology” provides guidance on institutional and procurement arrangements and risk-mitigation methodology for acquiring and managing public cloud solutions using a whole-of-government approach (World Bank 2023).

## **DATA STRATEGIES AND CLASSIFICATION FRAMEWORKS**

Because of data’s nonrivalrous nature, they can be shared among different stakeholders, resulting in repeated reuse to unlock the full potential of data and generate new insights. Data strategies across economies emphasize the importance of leveraging data through data sharing. In 2017, Rwanda introduced a National Data Revolution Policy that mandates open data publishing by public and private entities and emphasizes the importance of breaking down silos in government around data management. In Germany, data are estimated to create US\$458 billion in value, but 90 percent of that potential remains untapped. In 2021, the German government released its first Data Strategy, which highlighted the importance of establishing a connected data infrastructure and a program to promote high-performance computing. The strategy contained approximately 240 measures along four action lines: (1) making data infrastructure efficient and reliable; (2) increasing innovative and responsible data usage; (3) increasing data literacy and establishing a data culture; and (4) having the public sector lead by example. Similarly, the Dutch government released the Dutch Vision on Data Sharing between Businesses (Netherlands, Ministry of Economic Affairs and Climate Policy 2019) to promote business-to-business data sharing in 2019, and Australia’s Data Strategy charts a course to transforming the nation into a modern data-driven society by 2030 (Australia, Department of the Prime Minister and Cabinet 2021). Saudi Arabia’s National Strategy for Data & AI<sup>2</sup> aims to position the country as a global leader through investments, workforce development, and regulatory measures to nurture a thriving domestic ecosystem.

To facilitate data sharing, a data classification framework complements a management information system and a data architecture that facilitates shared data access. A data classification framework categorizes information by sensitivity level to ensure proper handling of data, reducing organizational risk. Information classification is based on the potential impact to national interest, organizations, or individuals should a breach of confidentiality,<sup>6</sup> integrity,<sup>7</sup> or availability<sup>8</sup> of classified information occur (Stine and others 2008).

Data classification policies have a direct bearing on cloud computing adoption. Fewer levels of classification and clear distinctions between levels ensure that the most sensitive information is properly secured.

The National Institute of Standards and Technology in the United States recommends using three categories: minimal impact, moderate impact, and high impact (Tierney 2023). The US government has adopted a three-tier classification scheme for national security information.<sup>2</sup> This scheme classifies data by the potential impact to national security in case of a data breach. In 2014, the UK government reduced its six levels of data classification to three: official, secret, and top secret. With this new classification system, over 90 percent of UK government data were labeled “official,” which meant that they could be stored without any restrictions in the public cloud,<sup>10</sup> and only the remaining 10 percent required hybrid or private cloud environments.

## CLOUD DEPLOYMENT BY GOVERNMENTS

Governments should carefully consider the public, private, hybrid, or multicloud deployment models and select the approach that best responds to their needs. In practice, a combination of two or more deployment models may be more suited than any one model. Many countries with cloud-first policies also have a government cloud established for data classified as unsuitable for public clouds. Singapore launched its Commercial Cloud First Policy in 2018 with an aim to migrate at least 70 percent of the government’s less sensitive information and communication technology systems onto the public cloud by 2023 to save costs. However, the government has also created a private cloud, called “G-cloud,” to meet security and governance requirements. Singapore’s G-cloud and its public cloud deployments are interoperable, allowing government agencies to use public cloud services for many needs.

A government cloud is an isolated private or community cloud computing environment designed to meet the needs and unique requirements of government agencies and organizations. Many government agencies worldwide prefer maintaining control over a sizable portion of their data, which is a reason private clouds remain attractive (van der Meulen 2018). Government clouds are owned, operated, and maintained by government entities or authorized contractors. Access to government cloud resources is typically restricted to government agencies, and in some cases to authorized partners or contractors that work with the government and host sensitive government data and applications. Examples of government cloud (in countries with no formal cloud-first policies) include the government private cloud in South Africa<sup>11</sup> and the Uzbekistan Cloud,<sup>12</sup> both developed with the primary purpose of serving the public sector. Japan’s Digital Agency took steps to establish a government cloud for the Japanese public sector by contracting several cloud service providers.<sup>13</sup> The Republic of Korea also partnered with five local technology companies to roll out the private cloud customized for the government’s use in 2022 (Lee 2022).

Some cloud providers offer dedicated cloud services tailored to government customers. Although not as versatile as public clouds, these dedicated private clouds have distinct advantages in terms of security, data privacy, and compliance with regulations. Several US federal agencies use cloud service designed by Amazon Web Services (AWS) for the US intelligence community.<sup>14</sup> Standard services were extended by introducing a “Top Secret” data center region designed for handling a full range of data, including data classified as top secret. This specialized data center region is accessible to the intelligence community and other government clients, provided they have the necessary secret-level network access and their own contractual agreements with AWS (Peterson 2021).

Multicloud deployments are becoming prevalent among government agencies. Australia (DTA 2021), Canada (Forrester Consulting 2022), New Zealand,<sup>15</sup> and the United States all support the use of multicloud deployments. Among low-income economies, Rwanda has adopted a multicloud strategy after first deploying a private cloud environment and subsequently moving to hybrid cloud deployments. Rwanda has developed a state-of-the-art data hosting facility, known as the National Data Center (AOS Ltd.) that caters to both private and public sector organizations. This center primarily serves as a repository for government data. Rwanda has also entered partnerships with several public cloud providers. Although multicloud solutions offer governments multiple advantages, Rwanda’s experience offers the important lesson that these solutions can also be quite challenging to implement, particularly in countries or regions with limited knowledge or skills for managing such environments. Box 6.4 discusses the migration of another country, Ukraine, to a multicloud environment.

#### **BOX 6.4** Ukraine’s migration to the cloud

In February 2022, the Ukrainian Parliament passed a Law on Cloud Services that enabled cloud-based backup of computer servers and data centers and the relocation of critical data to a public cloud environment. On March 12, 2022, the Ukrainian Cabinet of Ministers, in Resolution #263, permitted the placement of state information resources and public electronic registers on cloud resources or in data processing centers located outside of Ukraine. The successful migration effort involved more than 100 state and critical information registries, achieved through close collaboration with leading tech giants such as Amazon Web Services, IBM, Microsoft Azure, and Oracle. Many Ukrainian physical server farms were destroyed during the Russian Federation’s invasion of Ukraine; however, because of the transfer of vital data to secure cloud environments, information has remained accessible and protected. Ukraine’s Ministry of Digital Transformation says this experience underscores that digital resilience can be fostered beyond national boundaries and should be grounded in robust international cooperation and public-private partnerships.

*(Continued)*

**BOX 6.4 Ukraine's migration to the cloud (Continued)**

Currently, there is significant uncertainty regarding whether future Ukrainian cloud legislation will permit the use of overseas clouds. The Cabinet of Ministers' Resolution #263 allows government institutions to use overseas clouds for six months after the martial period ends and allows the banking sector to do so for two years. Government and banking institutions have enjoyed the benefits of using cutting-edge cloud technologies and services. In many cases, they have developed new services and functionalities atop these cloud platforms. For some, reverting back could result in operational degradation of services and could even jeopardize data integrity. Shifting from the cloud back to on-premises or a different environment also has the potential to disrupt ongoing operations. Planning for minimal disruption and the uninterrupted provision of critical services is crucial.

Therefore, any such data transfer and reintegration into on-premises systems or a different cloud environment would require meticulous planning, including managing potential complexities in data mapping, transformation, and compatibility checks. Potential changes during data's cloud tenure will make it important to address data consistency and synchronization, and they could present a challenge in reconciling data being brought back. Evaluating the compatibility of technologies between cloud environments and on-premises systems is vital because differences in architecture among applications, software, and tools used in the cloud could pose technical obstacles. Ensuring data security and privacy remains paramount during the transition, necessitating the safeguarding of sensitive data and adherence to relevant data protection regulations. Moreover, accounting for potential data loss or corruption is imperative, given the inherent risks associated with data migration processes. Thus, safeguards must be implemented to prevent data loss and maintain data integrity throughout the transition process.

If future legislation permits the use of overseas or European Union sovereign clouds for less critical data, Ukrainian law will need to establish a more refined data classification framework that ensures the protection of personal data.

Ukraine's Ministry of Digital Transformation is currently developing a cloud strategy that will envision future use of the public cloud environments after Russia's invasion of Ukraine ends. Given the absence of a legal and regulatory framework for cloud computing before the invasion, Ukraine is creating a framework informed by its unique needs and experiences.

*Source:* Box prepared by the Ministry of Digital Transformation of Ukraine.

Some governments are beginning to adopt a combined hybrid and multicloud approach. The Swiss government is actively pursuing such a strategy to integrate its in-house data centers and federally owned private clouds with public cloud services from various providers.<sup>16</sup> Similarly, the Malaysian government has adopted a deployment model that combines private cloud infrastructure with multiple public cloud environments (Red Hat 2023). Additionally, the European Commission has adopted a cloud-first approach with a hybrid multicloud service offering at the core of its cloud strategy (European Commission 2019).

After choosing a cloud deployment model, the government must next plan for cloud migration. Cloud migration is a complex task and needs a well-structured approach given multiple information systems and classifications. Migrating government information systems to the cloud involves a multistage process with several steps to ensure a secure and compliant migration. The steps in the migration process are interdependent, and each step requires careful planning and implementation: the decisions and actions taken at one stage affect the choices made for subsequent stages.

The first step is to identify all existing information systems available across government entities, by collecting and analyzing data from eligible agencies and producing a list of all systems and allied metadata. Each information system is then evaluated for cloud migration readiness. It is important to assess any risks or challenges that may arise during the migration process to avoid delays, additional costs, or performance problems. Several tools—such as the Cloud Migration Readiness Index (from Microsoft) and the Migration Readiness Assessment (from AWS)—can assist with migration readiness evaluation.

Once the evaluation is completed, information systems are classified and prioritized by their strategic importance, migration costs, and associated risks. A migration strategy is then determined for each information system, with strategies ranging from “lift and shift” migration, in which the systems are moved with minimal changes, to a full redesign of the system.

Continuously monitoring the process can ensure that it runs according to plan and helps respond to potential issues early on. Cloud migration is usually a multiyear effort and can be affected by technological and legal changes as well as emerging government priorities. Once the migration is complete, migrated information systems are verified before being available to more users. Box 6.5 outlines the process of Romania’s cloud migration.

**BOX 6.5 Romania's approach to identifying and prioritizing public sector applications and services for migration**

As part of its national recovery and resilience plan, the government of Romania decided to migrate the information systems of government institutions to the government cloud. The following main stages of the cloud migration were identified, all of which contribute to the ultimate objective of preparing the information systems for a secure and efficient transition to the cloud:

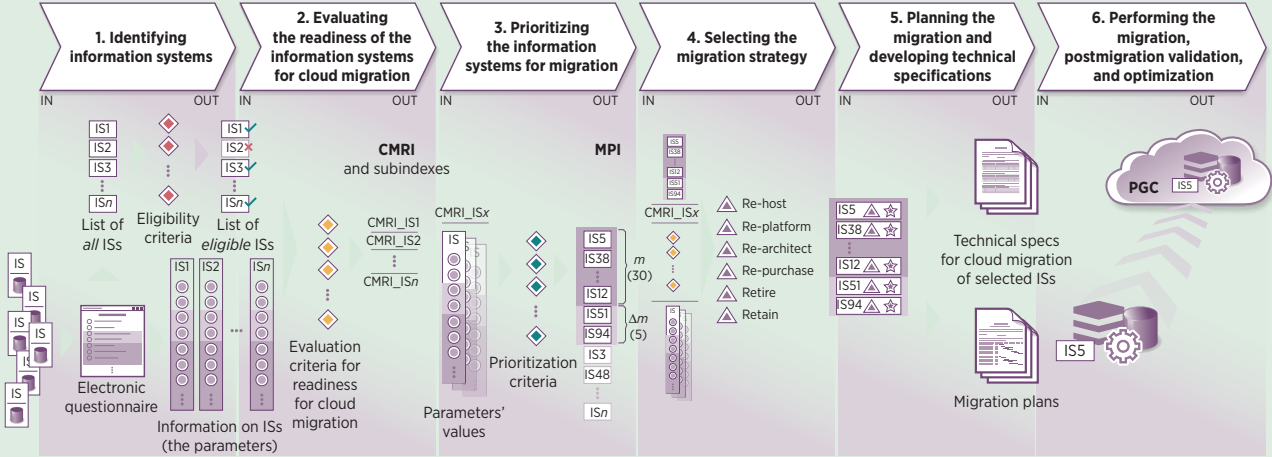
- *Identifying eligible information systems.* This stage includes collecting and analyzing data on the existing information systems of public authorities, with the aim of identifying eligible systems and gaining a solid understanding of their characteristics.
- *Evaluating the level of readiness of eligible information systems for cloud migration.* At this stage, the identified information systems are evaluated against multiple criteria—including technical, security, operational, and financial aspects—to determine their readiness for operating in a cloud environment.
- *Prioritizing the information systems for migration.* Using results of the evaluation, the information systems are classified and prioritized for migration. This prioritization is based on several factors, including the strategic importance of the system, the expected benefits of migration, and the associated risks.
- *Selecting the migration strategy.* Depending on the results of the prioritization, a migration strategy is established for each system. This strategy can vary from a full redesign of the system to a “lift-and-shift” migration, in which the system is moved to the cloud with minimal changes.
- *Planning the migration of the information system and developing the technical specifications.* At this stage, the system and the organization prepare for migration. This preparation can include, for example, development of technical specifications, purchase of required migration services, change management, staff training, and implementation of necessary security measures.
- *Performing the migration and postmigration validation and optimization.* At this stage, the system is migrated to the private government cloud, with continuous monitoring to make sure that the process takes place as planned and that any emerging issues are properly managed. After the migration is complete, the system is validated to ensure that it operates correctly in the new environment. Furthermore, adjustments or optimizations can be performed to maximize the benefits of the cloud.

A fundamental aspect of the migration to the cloud is recognizing and understanding the interdependencies between the various stages of the cloud migration process. These stages are sequential and iterative, meaning that decisions and actions taken in one stage can significantly affect the success of subsequent stages (figure B6.5.1).

(Continued)

**BOX 6.5** Romania's approach to identifying and prioritizing public sector applications and services for migration (Continued)

**FIGURE B6.5.1** Overview of the cloud migration process, Romania



Source: World Bank, Reimbursable Advisory Services Agreement on “Advice to Develop the Government Cloud Platform and to Migrate Selected Public Digital Services to the Cloud” (P180766), 2023. Unpublished.

Note: The Cloud Migration Readiness Index (CMRI) reflects the readiness level of the information system (IS) for migration to the cloud. Although calculated at the evaluation stage, CMRI also serves as a prioritization criterion. The Migration Priority Index (MPI) then determines the system’s priority for the migration. Both indexes are also used in the migration strategy selection stage. PGC = Private Government Cloud.

## PROMOTING CLOUD ADOPTION IN THE PRIVATE SECTOR

Small and medium enterprises (SMEs) account for 90 percent of all businesses and more than 50 percent of global employment.<sup>17</sup> Adoption of digital technologies by these enterprises can boost productivity growth, generate more jobs, and reduce regional inequalities. Cloud technologies are an important enabler of enterprise digitization. They enhance productivity, lower information technology costs, and facilitate access to enterprise resource management solutions. Cloud-based solutions can optimize supply chains and influence a range of enterprise functions from production to predictive machine maintenance and training, to marketing and communications. However, cloud adoption rates among SMEs remain low in low-income countries (Haraguchi, Kamiya, and Rodousakis 2023) and are a persistent issue in the European Union (Hallward-Driemeier and others 2020). Start-ups of the digital economy are also important users of the cloud. Many start-ups use the cloud to benefit from an infrastructure that can absorb peak loads without having to invest themselves. They are important customers of the big cloud players, who compete to accommodate them by offering credits, betting on their future growth as a driver for their own development.

Therefore, government's role in promoting the digital transformation of businesses and enhancing digital capabilities and adoption across various sectors is crucial for driving national digitalization and fundamental for the formation of the demand in cloud computing. Governments commonly use initiatives such as supporting SMEs or specific industries in their digital journey, accelerating the growth of technology start-ups, and creating an enabling environment for digital innovations or introducing financial incentives for businesses to facilitate their transition into the digital realm. For instance, Singapore's SMEs Go Digital program aims to enhance the accessibility and affordability of cloud computing for SMEs in the country.<sup>18</sup> The United Arab Emirates' Ministry of Economy joined forces with AWS to launch the AWS Connected Community initiative to facilitate the digitalization of SMEs, helping them expand in both local and international markets (Zawya 2023). The Indian government is also actively promoting cloud adoption through its Digital India and programs through the Ministry of Micro, Small and Medium Enterprises (MSME) (box 6.6).

## DIGITAL WORKFORCE DEVELOPMENT

A skilled and trained public and private sector workforce able to use digital technologies complements digital transformation strategies and determines their success. Despite growing demand for cloud computing skills, a talent gap exists in both low- and high-income economies, which can benefit from government initiatives. Governments should double

**BOX 6.6 Indian government initiatives to increase the country's digitization**

Digital India is a flagship program with a vision to transform India into a digitally empowered society and knowledge economy. The program consists of three main pillars: (1) digital infrastructure, which focuses on increasing availability of reliable and secure internet connection and ensuring digital identity for every resident of India; (2) governance and services on demand, which focus on digital public services, seamlessly integrated across government agencies; and (3) digital empowerment, which focuses on digital literacy and enabling regulations with equitable resources for Indian citizens.

The Digital MSME program aims at digitally empowering micro, small, and medium enterprises and motivating them to adopt digital tools, applications, and technologies in their production and business processes so they can improve their competitiveness in domestic and global markets. It is designed to empower these enterprises through digital technologies such as enterprise resource planning solutions to achieve higher competitiveness, improved efficiency, and lower costs—leading to a digitized economy.

down on their efforts to address the talent gap and create a pipeline of skills and competencies (Peixoto, Kaiser, and Rakotomalala 2022).

Digital skills development initiatives can range from basic digital literacy training to training in advanced digital technologies, including cloud computing and management of cloud applications. Many governments are launching digital academies as a starting point. Thailand's Digital Government Academy offers training, seminars, and other activities to upskill civil servants and promote digital skills awareness. In addition, the Thailand Government Big Data Institute has trained more than 1,000 government officers on data analysis and management skills (Sharon 2019). In the United Kingdom, the Government Digital Service helps public agencies improve citizens' digital services and offers training and skills development initiatives for civil servants (Cunnington 2017). As of 2023, the service had trained more than 7,500 civil servants.

Private sector partnerships can help address the skill gaps faced by government agencies and ensure that staff at all organizational levels have appropriate digital skills. In such partnerships, a private sector partner provides direct skills training or helps governments identify technology skills in high demand at present or in the foreseeable future. The Indian government partnered with the private sector to deepen cloud computing capabilities of public servants (Dharmaraj 2019) and trained them on the government's cloud adoption journey. The Singaporean government partnered with the private sector to deepen the data analytics and visualization techniques of public servants to help drive data-driven decisions (DSAITrends Editors 2020).

Cloud computing certifications and other capacity-building programs offered by cloud service providers can also be tapped as reskilling opportunities. Major private sector players—AWS, Cisco, Google Cloud, and Microsoft—and others offer certification courses.

Governments may find it more challenging to attract and retain talent because highly skilled technical employees may move to technology firms or start-ups. To retain and expand the talent pool, governments may need to review and revise their recruitment practices. Singapore revised its recruitment and talent development scheme to align with private sector salaries, and initiated recruitment of Singaporeans residing abroad. The government also introduced an initiative to reduce employee turnover among high-skilled technology talent, allowing them to engage with several public agencies to enhance their job satisfaction (Abell, Husar, and Lim 2022). For some low-income economies, public budgetary constraints might make it challenging to compete with the private sector. In these instances, governments may find it more viable to partner with the private sector to bridge skills gaps and broaden the talent base.

## NOTES

1. For an explanation of the differences between digitization, digitalization, and digital transformation, refer to chapter 3, “Assessing Digital Transformation Progress,” in the Organisation for Economic Co-operation and Development’s *Digital Transformation of National Statistical Offices* (OECD 2022).
2. MIT Technology Review, “Global Cloud Ecosystem Index 2022,” <https://www.technologyreview.com/2022/04/25/1051115/global-cloud-ecosystem-index-2022/>.
3. World Bank, “National Digital Transformation Strategy—Mapping the Digital Journey,” <https://digitalregulation.org/national-digital-transformation-strategy-mapping-the-digital-journey/>.
4. Denmark, “Guide on the Use of Cloud Services,” <https://en.digst.dk/digital-governance/new-technologies/guide-on-the-use-of-cloud-services/>.
5. Saudi Data & AI Authority, “National Strategy for Data & AI,” <https://ai.sa>.
6. Confidentiality means limiting of access to information to authorized persons for approved purposes.
7. Integrity means assurance that information has been created, amended, or deleted only by the intended authorized means and that the information is correct and valid.
8. Availability means ensuring timely and reliable access to and use of information.
9. National Archives, The President Executive Order 13526, <https://www.archives.gov/isoo/policy-documents/cnsi-eo.html>.
10. AWS, “Data Classification Models and Schemes,” <https://docs.aws.amazon.com/whitepapers/latest/data-classification/data-classification-models-and-schemes.html#u.s.-national-classification-scheme>.
11. SITA, “Cloud Computing,” <https://www.sita.co.za/content/cloud-computing-0>.
12. Huawei Cloud, “Uzbekistan Government Cloud,” <https://www.huawei.cloud.com/eu/cases/uzbekistangovernmentcloud.html>.

13. E-Learning, "Japan's Digital Agency Adopts AWS for Advance 'Government Cloud' Projects," <https://www.e-learning.asia/news-topics/nt2021102701/>.
14. AWS, "Cloud Computing for U.S. Intelligence Community," <https://aws.amazon.com/federal/us-intelligence-community/>.
15. New Zealand Government/Te Kawanatanga o Aotearoa, "All of Government Cloud Sourcing Strategy," <https://dns.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/cloud-adoption-policy-and-strategy/all-of-government-cloud-sourcing-strategy/>.
16. Swiss Federal Chancellery FCh, "Cloud," <https://www.bk.admin.ch/bk/en/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html>.
17. World Bank, "Small and Medium Enterprises (SMEs) Finance," <https://www.worldbank.org/en/topic/smefinance>.
18. Infocomm Media Development Authority, "SMEs Go Digital," <https://www.imda.gov.sg/how-we-can-help/smes-go-digital>.

## REFERENCES

- Abell, Thomas, Arndt Husar, and Lim May-Ann. 2022. "Cloud Computing as a Key Enabler for Digital Government across Asia and the Pacific." ADB Sustainable Development Working Paper 77, Asian Development Bank. <https://www.adb.org/sites/default/files/publication/707786/sdwp-077-cloud-computing-digital-government.pdf>.
- Australia, Department of the Prime Minister and Cabinet. 2021. *Australian Data Strategy: The Australian Government's Whole-of-Economy Vision for Data*. Government of Australia. <https://www.finance.gov.au/sites/default/files/2022-10/australian-data-strategy.pdf>.
- Cunnington, Kevin. 2017. "The Government Transformation Strategy 2017 to 2020." *UK Government Digital Service* (blog), February 9. <https://gds.blog.gov.uk/2017/02/09/the-government-transformation-strategy-2017-to-2020/>.
- Dharmaraj, Samaya. 2019. "Digital Governance Tech Tour to Boost Digital India." *OpenGov*, August 28. <https://opengovasia.com/digital-governance-tech-tour-to-boost-digital-india/>.
- DSAITrends Editors. 2020. "GovTech Continues Push to Deepen Data Skills in Singapore's Public Service." *CDO Trends*, July 15. <https://www.cdotrends.com/story/14947/govtech-continues-push-deepen-data-skills-singapore-s-public-service?refresh=auto>.
- DTA (Australia, Digital Transformation Agency). 2021. *Secure Cloud Strategy*. Commonwealth of Australia. <https://www.dta.gov.au/sites/default/files/2022-09/DTA%20Secure%20Cloud%20Strategy%20-%20October%202021%20v3.pdf>.
- Edward, Simon. 2024. "The State of the Cloud in Latin America." *Ascend Cloud Solutions* (blog), January 26, 2024. <https://www.ascendcloudsolutions.com/the-state-of-the-cloud-in-latin-america>.
- European Commission. 2019. "Cloud Strategy: Cloud as an Enabler for the European Commission Digital Strategy." European Commission. [https://commission.europa.eu.mcas.ms/system/files/2019-05/ec\\_cloud\\_strategy.pdf?McasCtx=4&McasTsid=15600](https://commission.europa.eu.mcas.ms/system/files/2019-05/ec_cloud_strategy.pdf?McasCtx=4&McasTsid=15600).
- European Commission. 2021. "2030 Digital Compass: The European Way for the Digital Decade." Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM 118, Brussels. [https://commission.europa.eu.mcas.ms/system/files/2023-01/cellar\\_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02\\_DOC\\_1.pdf?McasCtx=4&McasTsid=15600](https://commission.europa.eu.mcas.ms/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf?McasCtx=4&McasTsid=15600).

- Forrester Consulting. 2022. "Multicloud Is the New Frontier of Government IT." VMware. [https://www.vmware.com/learn/1380503\\_REG.html](https://www.vmware.com/learn/1380503_REG.html).
- Hallward-Driemeier, Mary, Gaurav Nayyar, Wolfgang Fengler, Anwar Aridi, and Indermit Gill. 2020. "Europe 4.0: Addressing the Digital Dilemma." World Bank, Washington, DC. <http://hdl.handle.net/10986/34746>.
- Haraguchi, Nobuya, Marco Kamiya, and Niki Rodousakis. 2023. "Boosting Digital Transformation for Sustainable Development." Newsletter of the UNIDO Industrial Analytics Platform, August. <https://iap.unido.org/articles/boosting-digital-transformation-sustainable-development>.
- Lee, Seung-Woo. 2022. "SK, Naver to Launch Cloud Services for Korean Public Institutions." *The Korea Economy Daily Global Edition*, July 21. <https://www.kedglobal.com/cloud-computing/newsView/ked202207210017>.
- Netherlands, Ministry of Economic Affairs and Climate Policy. 2019. *Dutch Digitalization Strategy: Dutch Vision on Data Sharing between Businesses*. Government of the Netherlands.
- OECD (Organisation for Economic Co-operation and Development). 2022. *Digital Transformation of National Statistical Offices*. Paris: OECD Publishing. <https://www.oecd-ilibrary.org/sites/a366b2b2-en/index.html?itemId=/content/component/a366b2b2-en>.
- Peixoto, Tiago Carneiro, Kai Kaiser, and Olivia Rakotomalala. 2022. "Governments Aren't Getting Enough Digital Skills." *Governance for Development* (blog), November 2. <https://blogs.worldbank.org/governance/governments-arent-getting-enough-digital-skills>.
- Peterson, Max. 2021. "Announcing Second AWS Top Secret Region, Extending Support for US Government Classified Missions." *AWS Public Sector Blog*, December 6. <https://aws.amazon.com/blogs/publicsector/announcing-second-aws-top-secret-region-extending-support-us-government-classified-missions/>.
- Public First. 2022. "Unlocking Europe's Digital Potential." Report commissioned by Amazon Web Services, Public First. <https://awsdigitaldecade.publicfirst.co.uk/>.
- Red Hat. 2023. "3 Hacks to Achieve Multi-Cloud and Hybrid Cloud Excellence." *GovInsider*, September 11. <https://govinsider.asia/intl-en/article/3-hacks-to-achieve-multi-cloud-and-hybrid-cloud-excellence>.
- Rubens, Paul. 2011. "The Government's Plan for the Cloud." Internet.com. <https://docs.broadcom.com/mcas.ms/doc/12380280?McasCtx=4&McasTsid=15600>.
- Say, Mark. 2020. "Scotland Declares 'Cloud First' for Public Sector." *UKAuthority*, June 10. <https://www.ukauthority.com/articles/scotland-declares-cloud-first-for-public-sector/>.
- Schijman, Agustina, Pablo Valenti, Carlos Pimenta, Aitor Cubo, and Fabiano Bastos. 2020. *Computación en la nube: Contribución al desarrollo de ecosistemas digitales en países del Cono Sur*. Inter-American Development Bank. <https://publications.iadb.org/es/computacion-en-la-nube-contribucion-al-desarrollo-de-ecosistemas-digitales-en-paises-del-cono-sur>.
- Sharon, Alita. 2019. "Thailand to Train Government Officers on Big Data Skills." *OpenGov*, December 17. <https://opengovasia.com/thailand-to-train-government-officers-on-big-data-skills/>.
- Stine, Kevin, Rich Kissel, William C. Barker, Jim Fahlsing, and Jessica Gulick. 2008. *Information Security. Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories*. NIST Special Publication 800-60 Volume 1, Revision 1, National Institute of Standards and Technology, Gaithersburg, MD. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf>.
- TeleGeography. 2021. "Argentina Country Profile." PriMetrica Inc.

- Tierney, Mike. 2023. "NIST 800-53: A Guide to Compliance." *Netwrix* (blog), March 3, updated on March 17, 2023. <https://blog.netwrix.com/2021/03/03/nist-800-53/>.
- United Kingdom, Central Digital and Data Office. 2021. *Cloud Guide for the Public Sector*. Government of the United Kingdom. <https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector>.
- United Kingdom, Government Digital Service. 2020. "How the Welsh Government Migrated Their Technology to the Cloud." Case Study, March 27. <https://www.gov.uk/government/case-studies/how-the-welsh-government-migrated-their-technology-to-the-cloud>.
- van der Meulen, Rob. 2018. "Understanding Cloud Adoption in Government." Gartner, April 11. <https://www.gartner.com/smarterwithgartner/understanding-cloud-adoption-in-government>.
- World Bank. 2023. "Institutional and Procurement Practice Note on Cloud Computing." *Equitable Growth, Finance and Institutions Insight*, World Bank, Washington, DC. <https://openknowledge.worldbank.org/items/7baff007-7bb9-4623-b229-b105cbf47284>.
- Zawya. 2023. "Ministry of Economy & Amazon Web Services to Support Digitization & Growth of SMEs in UAE by Leveraging the AWS Platform." Press Release, June 14. <https://www.zawya.com/en/press-release/companies-news/ministry-of-economy-and-amazon-web-services-to-support-digitization-and-growth-of-smes-in-uae-by-leveraging-the-aws-platform-c0brkgqq>.

