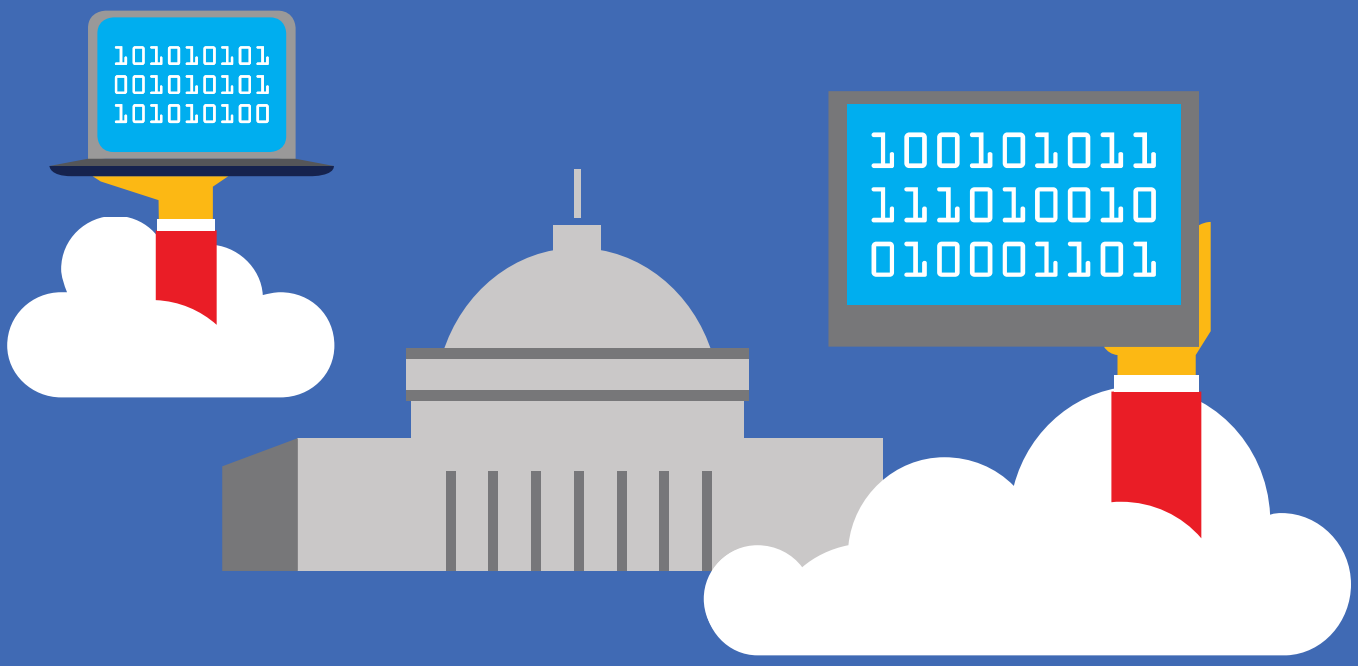
Microsoft

Transforming Government

Cloud policy framework for innovation, security, and resilience



Authors

Amanda Craig

Paul Nicholas

Contributors

Gregg Brown

Scott Charney

Kaja Ciglic

Scott Edwards

Cristin Goodwin

Min Hyun

James Kavanagh

Steve Mutkoski

Tyson Storch

Kevin Sullivan

Executive summary

Rapid advances in technology enable incredible productivity and dramatic progress in governments' and their citizens' abilities to communicate, innovate, and implement new ideas. Cloud computing illustrates this well, delivering broad benefits that far outpace anything imagined just a few years ago. Furthermore, cloud computing will be fundamental to future technology breakthroughs, delivering big data analytics and empowering the Internet of Things (IoT). However, new technologies also introduce new complexities and require a fresh assessment of how to best adjust to and optimize for their distinct challenges and opportunities.

Microsoft has long supported the notion that governments should develop a national strategy for cybersecurity to guide their effective management of challenges and opportunities in an era of information and communication technologies (ICT). In addition, Microsoft proposes a set of cloud security policy principles for governments' consideration. Our experience working with national and local governments around the world enables us to understand the unique challenges that they face as they adopt new technologies like cloud computing. We built on that knowledge to develop these principles, seeking to guide governments as they balance the benefits and risks of migrating to cloud platforms and solutions.

In particular, the principles in this paper focus on how to use cloud computing to achieve security and resiliency of government operations, a critical foundation of any technology implementation. These principles are grounded in what we believe to be best practices pursued by various governments that have already tested and trusted the cloud. They also build on the commitments that Microsoft puts at the heart of our trusted cloud: security of operations, data protection and privacy, compliance with local requirements, and transparency in how we do business. To optimize their effectiveness, the principles should be considered as part of a larger national approach, consistent with and incorporated into broader cybersecurity and ICT strategies and plans. Microsoft also hopes that this paper will encourage debate, information sharing, and best practice exchange between and amongst government entities for years to come.

Transforming government is the first in a series of cloud security policy publications, introducing cloud security concepts. Future publications will, amongst other things, discuss how to approach and implement data classification and governance, how to assess and mitigate cybersecurity risks in cloud computing, and how to structure policy decisions and responsibilities so that constant iteration and improvement are embedded within government processes. With this series, Microsoft seeks to enable governments to take advantage of cloud computing, unlock innovation potential in their countries, and improve the security and resiliency of their services.

Table of contents

Executive summary 1

Table of contents 2

Introduction 3

Why choose cloud computing? 4

Public policy principles for cloud innovation, security, and resilience 8

- Innovative 9
- Flexible 11
- Data-aware 13
- Risk-based 15
- Standards-based 17
- Transparent 19

Conclusion 21

Introduction

ICT can have enormous transformative power, connecting people as they share ideas, solve problems, and pursue opportunities for discovery and growth. Throughout history, governments and societies have witnessed such transformations as they have worked toward improving how information is shared, resolving inevitable challenges as they have arisen. Nearly two centuries ago, for instance, countries devised a system to ease the transmission of telegrams across national borders, standardizing the technology for their mutual use through a new institution. The telegram changed the speed with which governments were able to communicate forever; near real-time information had the potential to change the course of battles for the first time, in either the intended receiver's or an interceptor's favor.

In the 20th century, technology marched on, again demonstrating its transformative power for governments and societies. Reliable international telephone services were established, creating opportunities for government leaders to have ongoing conversations directly and making the world seem smaller and more secure. The iconic "red telephone" served as an important connection between world leaders in Russia and the United States during the Cold War. Then, the global Internet became mainstream, profoundly changing almost every aspect of modern life. The Internet suddenly made the world seem even smaller and vastly more complex. The Internet also kick-started many other innovations, including cloud computing, the technology that's changing the world today.

Cloud computing will unleash a whole new generation of transformation. Governments that successfully implement cloud computing will not only be able to deliver efficient and cost-effective services but also will earn innovation, security, and resiliency dividends. However, understanding how to make the right policy, operational, and procurement decisions can be difficult with any new technology, and doing so can seem especially daunting with cloud computing because it has the potential to alter the paradigm of how business is done. More specifically, confusion about appropriate legislative frameworks and specific security requirements of different data assets risks slowing government adoption.

Cloud computing is an unavoidable reality for 21st century governments around the world. To support government transitions to cloud technology and advance government innovation, security, and resiliency, Microsoft offers six cloud security policy principles to guide the next generation of ICT policy.

Cloud computing in emerging economies[1]

Cloud computing offers tremendous opportunity for emerging economies. Although broadband infrastructure challenges must be acknowledged and resolved, cloud computing is, in many ways, the ideal option for emerging economies. It allows significant flexibility in the choice of terminal device that links the user to information applications, so consumers can access data-intensive applications on mobile devices, the prevalent choice for connecting to the Internet in the developing world. In addition, cloud computing is adaptable and scalable, allowing organizations and individuals to access computing and educational resources that they would otherwise not be able to reach. For instance, cloud-based learning materials might be shared amongst schools, universities, libraries, or other organizations. These aspects of cloud computing are also foundational to encouraging an entrepreneurial culture, especially one that can enable a new range of ICT service offerings.

1 *Security Framework for Governmental Clouds*. European Union Agency for Network and Information Security (ENISA). February 2015. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds/security-framework-for-governmental-clouds/at_download/fullReport

Why choose cloud computing?

Cloud computing represents a seismic shift when compared to traditional computing, enabling governments to do more, faster. In part, this shift is due to the way in which cloud services are provisioned and maintained, reducing the burden on users to install and update hardware and software. In short, cloud computing customers can tap into the power of datacenters and services without having to build, manage, or maintain them. Moreover, shared or managed responsibility for patching means that every time there is a new release or update, cloud customers save both time and money and increase security automatically.

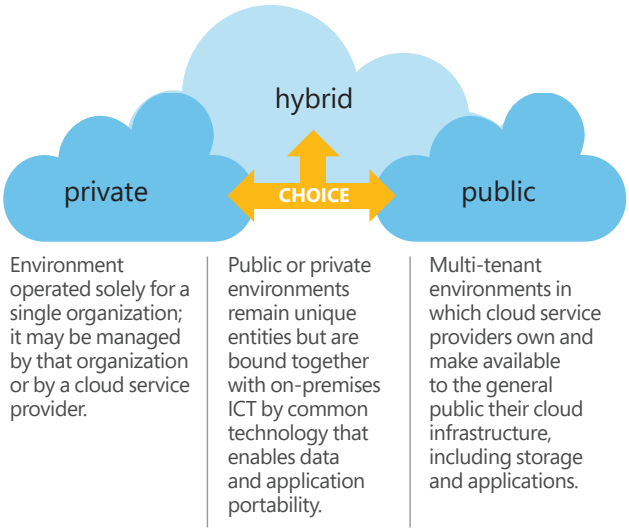


Image 1: Public, private, and hybrid cloud deployment models

Various cloud computing deployment options are possible. Cloud environments can be public, private, or hybrid, and the drawbacks and benefits vary with each model. For instance, the actual costs of public cloud are relatively low because the public cloud environment benefits from economies of scale, meaning that providers' physical and virtual computing resources are pooled and then assigned and reassigned to serve multiple consumers.[2] As a result, customers sharing distributed resources achieve a lower variable cost than they could access on their own. A private cloud shares many of the characteristics of public cloud computing, including self-service, elasticity, and pay-by-use, in addition to dedicated resources that provide additional control and customization. The hybrid cloud merges the best of both worlds, allowing customers to move between public cloud, private cloud, and traditional on-premises environments.

In addition to various deployment models, there are also numerous cloud services options, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). As with the cloud deployment models, the cloud services options have differing benefits and drawbacks.[3] Whereas IaaS solutions allow for optimum flexibility, providing computing power to support various software programs, SaaS solutions offer ready-made but less flexible programs. SaaS solutions are the easiest to manage, requiring that cloud providers take on a greater degree of responsibility over the implementation of various security controls, and IaaS solutions require cloud customers to continue to manage more security implementations. In both instances, PaaS offers a middle ground, providing a platform and tools to ease the creation and management of organization-specific software. Image 2 depicts the various control responsibilities that cloud customers and providers have in IaaS, PaaS, and SaaS environments.

2 Arora, Pankaj, Raj Biyani, and Salil Dave. *To the Cloud: Cloud Powering an Enterprise*. 2012.

3 *Software as a Service (SaaS)* is a software delivery business model in which a provider or third party hosts an application and makes it available to customers on a subscription basis. SaaS customers use the software running on the provider's infrastructure on a pay-as-you-go basis. Microsoft Online Services is an example of subscription-based, on-demand applications and hosted services, providing end users with a consistent experience across multiple devices.

Infrastructure as a Service (IaaS) is similar to traditional hosting, in which a business uses the hosted environment as a logical extension of the on-premises datacenter. The servers (physical and virtual) are rented on an as-needed basis, and the ICT professionals who manage the infrastructure have full control of the software configuration. Examples include Microsoft datacenters, which allow customers to scale with ease and speed to meet the infrastructure needs of the entire organization or of the individual departments within it, globally or locally.

Platform as a Service (PaaS) offers hosted application servers that have near-infinite scalability resulting from the large resource pools that they rely on. PaaS also offers necessary supporting services, including storage, security, integration infrastructure, and development tools for a complete platform. The Microsoft Azure platform may provide a PaaS, consisting of an operating system, a fully relational database, and consumable web-based services that provide security-enhanced connectivity and federated access control for applications.

Regardless of which deployment or service model is implemented, cloud computing can enable governments to increase the agility and efficiency of their operations and lower overhead costs of ICT.[4] In addition, new computing resources are just a click away, whereas traditional ICT solutions could take weeks or even months to stand up. Because resources are elastically provisioned, they can quickly scale, and users only pay for computing resources when they consume them. This can be particularly helpful for government services, such as e-government tax filings and returns, which experience a predictable spike in usage and capacity. Cloud computing also supports more rapid and fluid innovation, creating shared services, promoting iterative development, providing built-in analytics that take advantage of big data, and enabling employees to access resources from their own devices to collaborate on a global platform.

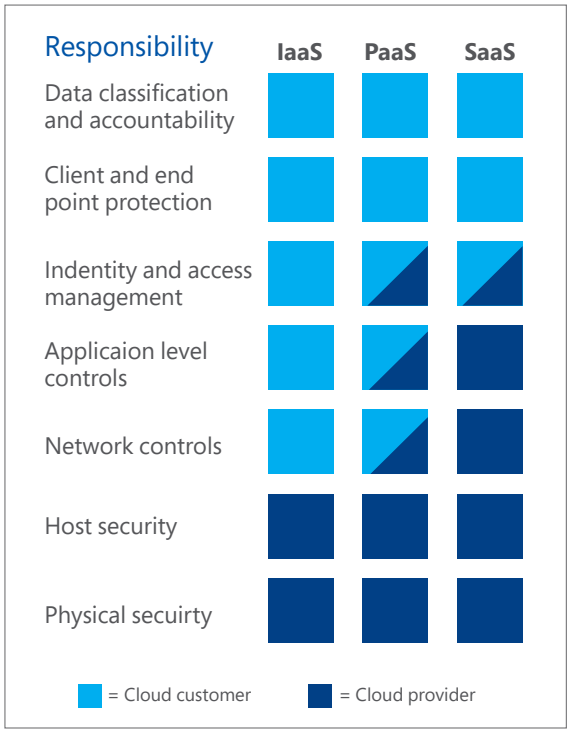


Image 2: Considerations for cloud service choice

Best practice: Taxpayers in Mexico benefitting from cloud adoption[5]

With the goal of continuing to improve the services offered to Mexican taxpayers, Mexico's Tax Administration Service (SAT) chose to deploy Microsoft Azure cloud computing services in 2014. Through Azure, the government agency took advantage of the elasticity of cloud computing services to help:

- **Issue electronic invoices;**
- **Provide direct customer support from the portal to all taxpayers who are required to check, cancel, or download electronic invoices issued by themselves or on their behalf; and**
- **Support more than 85 authorized certification providers with filing-related services.**

"Since we started using Microsoft Azure services with the SAT, we have processed close to 4 billion documents with the peace of mind that Microsoft Azure helps keep the information secure, which is fundamental for the organization," said Juan Manuel Galarza, General Administrator for Communications at the SAT. Azure has also allowed the agency to process daily peaks of up to 34 million electronic invoices.

4 *Value of Cloud Security: Vulnerability.* Leviathan Security Group. 2015. http://www.leviathansecurity.com/wp-content/uploads/Value-of-Cloud-Security-Vulnerability.pdf

5 Thomlinson, Matt. "Groundbreaking project assesses public cloud for a more resilient Estonia." Microsoft Cyber Trust Blog. February 4, 2015. http://blogs.microsoft.com/cybertrust/2015/02/04/groundbreaking-project-assesses-public-cloud-for-a-more-resilient-estonia/

Most importantly, cloud computing can increase the security and resilience of an organization's ICT infrastructure. In part, security improves because moving data and services to the cloud can act as a forcing function for robust data governance. As a result, organizations become not only more aware of the data that they retain but also more purposeful about how they treat it. A move to cloud services may also improve security because it transfers some responsibility for managing ICT onto the cloud service provider (CSP). Depending on the cloud service model, cloud providers may not only manage datacenter security but also network controls, identity and access controls, and patching. Large CSPs also have visibility into and the ability to quickly protect their entire environments. For instance, Microsoft detonates email attachments blocked by our advanced threat protection service,[6] and if malware is found in the attachment, then we can search our entire cloud environment for that attachment and protect all of our customers from that malware. Alternatively, if a government agency detects a new piece of malware in its environment, then to protect other agencies, it must share that malware, and other agencies must look for it—a much more tedious process.

In addition, large CSPs in particular see providing robust security and resilience as competitive differentiators and therefore invest heavily in the area. As a result, they often devote substantially more resources to improving ICT security than governments. According to the Organization for Economic Cooperation and Development (OECD), large CSPs *"are in the position to hire specialists for very specific security threats…"* and to *"dynamically upscale computing resources dedicated to security measures…"*[7] Moreover, their investments in advanced security measures go further, as large CSPs can more cost effectively provide security implementations such as physical access control or the overall application of security policy and maintenance processes. According to the European Network and Information Security Agency (ENISA), *"All kinds of security measures are cheaper when implemented on a larger scale,"* including filtering, patch management, hardening of virtual machine (VM) instances and hypervisors, threat management, and scaling of resources for traffic shaping and authentication.[8]

Some experts have also noted that rapid, smart scaling of distributed cloud resources results in resilience advantages, enabling large CSPs to thwart emergencies and distributed denial of service (DDoS) attacks more effectively than on-premises solutions.[9] Large CSPs utilize geographic replication, building databases in many locations around the world, which enables them to host relevant data or services in regions unaffected by local or regional emergencies. Therefore, if a government loses access to its on-premises servers due to an environmental disaster, political conflict, or other unforeseen crisis, public cloud services can continue to safeguard data or to support essential government services.

6 "Advanced threat protection for safe attachments and safe links." Exchange Online. 2015. https://technet.microsoft.com/en-us/library/mt148491%28v=exchg.150%29.aspx

7 *Cloud Computing: The Concept, Impacts and the Role of Government Policy.* Organization for Economic Cooperation and Development (OECD). August 19, 2014. http://www.oecd-ilibrary.org/science-and-technology/cloud-computing-the-concept-impacts-and-the-role-of-government-policy_5jxzf4lcc7f5-en

8 Catteddu, Daniele, and Giles Hogben. *Cloud Computing: Benefits, risks and recommendations for information security.* ENISA. December 2012. https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

9 Ibid.

Best practice: Estonia increasing resiliency of government services by using cloud computing[10]

For more than a decade, Estonia has taken a particularly innovative approach to e-government. Today, Estonians are able to perform many public and private sector transactions online. Moreover, the authoritative version of many essential government registries is digital, and many documents only exist in digital form. As a result, resiliency and security of government services are critical to the country.

The Estonian government is therefore committed to incorporating the latest secure technologies available into its ICT systems, proactively phasing out any ICT systems that are approaching their end of life. Through a Virtual Data Embassy pilot with Microsoft, the government has also examined the use of public cloud services to ensure the country's digital continuity. The pilot used Azure to test the security and resilience of the Estonian president's website (www.president.ee) and the country's law registry (www.riigiteataja.ee), ultimately finding that the Estonian government should utilize cloud computing to increase the security and resilience of its infrastructure and services. Moreover, the pilot's results led to a recommendation that an overarching cloud strategy and government action plan facilitating cloud migration should be developed to enable technical and operational agility and to increase cost effectiveness.

Cloud computing offers governments multiple potential benefits, including cost savings, innovation opportunities, and increased efficiency, agility, security, and resilience. However, moving to the cloud is not without security, resilience, and other challenges. Cloud computing can be "both a friend and a foe," just as with on-premises ICT systems.[11] For example, both may pose data protection and malicious insider challenges. Moreover, some customers may perceive cloud services as posing new challenges resulting from loss of ICT control, although ENISA has noted that such concerns may be mitigated by awareness, transparency, and contractual agreements.[12] In addition to providing transparency to our customers by sharing information about our security processes and through tools like access to their data and audit logs, Microsoft seeks to shift control back to cloud consumers through services like Office 365 Lockbox and choices like determining where data resides.[13] Understanding cloud computing security, resilience, and related challenges and how to manage them within in a government context are the primary objectives of the policy framework that follows.

10 Thomlinson, Matt. Op cit.

11 Catteddu. Daniele. Op. cit.

12 *Good Practice Guide for securely deploying Governmental Clouds.* ENISA. November 15, 2013. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/good-practice-guide-for-securely-deploying-governmental-clouds

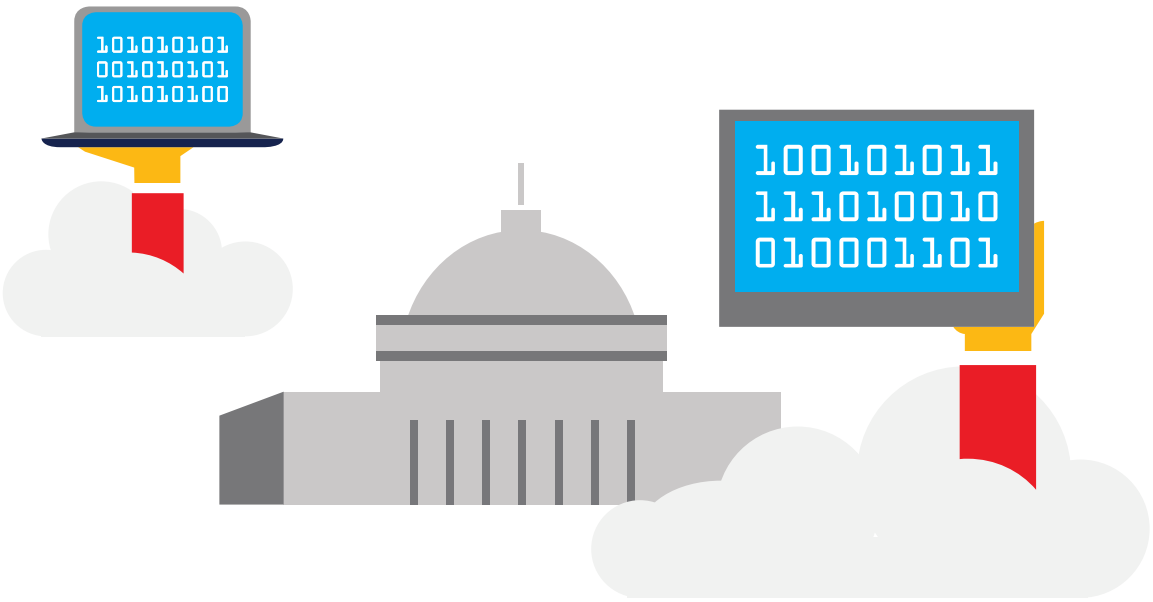
13 "Announcing Customer Lockbox for Office 365." Office Blogs. April 21, 2015. https://blogs.office.com/2015/04/21/announcing-customer-lockbox-for-office-365/

Public policy principles for cloud innovation, security, and resilience

Cloud policy prinicples

1. Innovative
2. Flexible
3. Data-aware
4. Risk-based
5. Standards-based
6. Transparent

The six principles outlined in this section provide a framework for government ICT decision-makers. The principles are designed to provide helpful guidance to policy makers as well as ministries and various departments as they begin to implement procurement guidelines for cloud computing. As such, the principles are intentionally written at a high level to account for various implementation approaches in different cultural and technological environments. The paper also provides examples of the principles in action. In particular, best practices and examples from around the world have been highlighted to encourage inter-governmental partnership and exchange of ideas. Ultimately, these six principles create a foundational framework that governments can utilize as they develop 21st-century policies to transform government, advance the security and resiliency of their services, and spark more innovative digital societies.



1 Innovative

PRINCIPLE: Cloud policies should set a clear path toward innovating and advancing the security and resiliency of their government services.

When organizations make investment decisions about a particular technology, they typically assess its adoption along several different criteria, such as whether the new system will help them boost productivity, move beyond critical challenges, raise their innovative potential, or lower the cost of their ICT infrastructure. For governments in particular, the potential impact of improved digital services on the wider economic development of the country may also be an important consideration. Likewise, using new technology to increase security can have wide-ranging effects on the online security of the country as a whole. This is particularly important in the context of transformative technologies like cloud computing because societies at the forefront of such transformations can benefit from being able to affect their evolution.

To achieve their objectives, governments must make intentional choices about when and how to utilize modern ICT systems and services. The pace at which they incorporate innovation must be directly connected to the realities of their environments, and how they choose to use available resources and to plan for the future should be carefully assessed. One consideration that should drive their decision-making is preservation of the market's ability to innovate and compete to deliver the best solutions, including in security. Governments can also use their purchasing power to drive change and innovation in their domestic and international economies much more effectively than they can by deciding to develop their own solutions.

Best practice: London commuters using open data and cloud services to innovate and increase resiliency[14]

Since 2011, Transport for London (TfL) has worked with Microsoft to use London's available open data to provide better services to its customers—whether they are on the rail or on the road. Since the Azure deployment, the London Underground Trackernet system has gone from receiving 1,000 hits a day to 2.3 million. Even with bad weather and major events in London, Azure scales to meet the spikes in demand without increasing the strain on the TfL server. Open data is also used in the bicycle rental program, ensuring that, at any particular time, customers know where bicycles are available in the city.

The partnership has also resulted in the continuous addition of innovative solutions, including most recently contactless payment for travelers on the London Underground. The payment solution, called Contact Assistant, runs separately from the general Oyster payment card system. With the Oyster card system, most of the billing information is held on the actual cards, which have limited capacity. However, Contact Assistant data is held centrally on a Microsoft SQL Server system, which runs a new billing engine. One immediate advantage for passengers is that the Contact Assistant system technology makes weekly fare capping possible, allowing passengers to travel as much as they like in a single day or week and limiting the amount that they pay for this travel. As such, these innovations support not only greater ease of use for transit riders but also increased security and resiliency, enabling them to be successful.

14 Stanchak, Jesse. "Transport for London: Making contactless payment flawless." Microsoft Enterprise Home. April 6, 2015. https://www.microsoft.com/en-gb/enterprise/it-trends/cloud-computing/articles/transport-for-london-making-contactless-payment-flawless.aspx#fbid=JdaFjVkwR-A

Microsoft encourages governments to take a forward-leaning, proactively innovative approach, recommending that their various government entities actively assess whether to procure cloud services by adopting a "cloud first" policy. A number of countries have already taken a similar approach, including Australia, the United Kingdom, and the United States.[15] Cloud first policies represent an important policy-setting tool; they not only empower government entities to implement cloud computing solutions when appropriate but also encourage the development and implementation of an assessment process, which allows for careful evaluation of governmental goals and requirements for adoption of cloud services.

This evaluation process is particularly important in the context of security and resilience of government systems. Although cloud computing can greatly simplify ICT management, making it an appealing option for often overburdened and under-budgeted governments, security remains a pivotal consideration for government ICT purchasing. As such, cloud first policies must set in motion the evaluative activities that will ultimately facilitate secure and resilient technical and operational migration. Part of that process, as highlighted in the "Data-aware" principle below, requires that governments take steps to increase internal awareness of their data and services and understand associated levels of risk for each data set or service. In addition, as part of their evaluative processes, governments should ensure that they can continuously access the newest security and resiliency innovations and put them to use to protect and provide better services for their citizens. By setting a clear path toward innovation and thoughtful evaluation, governments will empower their ministries to take advantage of the many benefits of cloud computing, including increased security and resiliency.

15 *Australian Government Cloud Computing Policy: Smarter ICT Investment.* Australian Government Department of Finance. 2014. http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf; Government cloud strategy. United Kingdom Cabinet Office and Efficiency Reform Group. October 27, 2011. https://www.gov.uk/government/publications/government-cloud-strategy; Kundra, Vivek. *Federal Cloud Computing Strategy.* The White House. February 8, 2011. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

2 Flexible

PRINCIPLE: Cloud policies should be flexible and should enable governments to select the most suitable cloud types for delivering their services in a secure and resilient manner.

Cloud policies play a vital role in setting the boundaries within which different government entities can adopt cloud technologies. A number of governments have already developed national cloud strategies that define various cloud services and deployment models, and some also consider in what contexts the different services might be appropriate. In providing such definitions and contexts, policy makers have often relied on guidance from an authoritative source, such as the National Institute for Standards and Technology (NIST) or ENISA, which have in turn developed guidelines in this space.[16] A coordinated national strategy can therefore support various government entities' implementation of cloud services, sharing information about the various possible cloud deployment models and services and helping to ensure that necessary legal, technical, and policy requirements are met.

Security and resilience frequently feature prominently in these national strategies, acknowledging challenges that governments face not only in outlining security considerations for new and emerging technologies but also in developing ways to respond to such considerations. Some governments propose specific security certification frameworks, the development of such, or the implementation of risk management baselines for government entities and critical infrastructures. Others put forward potential frameworks for conducting risk assessments or develop and use model contracts, which focus on achieving a high level of security.

Although Microsoft supports this approach, recognizing that great efficiency is achieved by government coordination in developing and using security baselines or model contracts, we also recommend that government entities retain sufficient flexibility as they develop and implement their local cloud security policies. This will ensure that they can apply their knowledge and hands-on experience to make the best decisions for their environments. Governments can achieve this flexible approach by defining key security and resiliency baselines that agencies should meet but then allowing agencies to match the specifics of technology and deployment to their own needs, incorporating compliance requirements that are driven by the particular data and services that they are migrating to the cloud. For example, incorporating and following the flexible principle would allow for different treatment of different data—depending on its sensitivity levels.

16 Australian Government Department of Finance. Op cit.; *Prescribing the Philippine Government Cloud Computing Policy*. Department of Science and Technology. 2013. http://i.gov.ph/govcloud/govcloud-policies/draft-memorandum-circular-prescribing-philippine-government-cloud-computing-policy-june-13-2013/; *Cloud Security Policy for Government Agencies*. Qatar Ministry of Information and Communication Technology. 2014. http://www.ictqatar.qa/en/file/13596/download?token=W7K0iaUM. See also NIST Definition of Cloud Computing. http://www.nist.gov/itl/csd/cloud-102511.cfm; and Catteddu, Daniele, Op. cit.

Best practice: Australia driving flexible cloud procurement decision-making[17]

In 2014, the Australian Department of Finance published the "Australian Government Cloud Computing Policy Version 3.0." The policy is mandatory for all government agencies, and it underlines the government's commitment to accelerating the adoption of cloud services. It is accompanied by a number of guides to help government departments think through the procurement process, including resource management, financial, and legal guides, along with guides specifically dealing with privacy and security.

The 2014 policies were also significant because the government took steps to ensure that the cloud security assessment process would be more flexible, context-dependent, and streamlined. Whereas the attorney-general's department was previously required to approve any movement of data offshore, since the 2014 policy changes, departments have the power to implement their own risk management processes and to make decisions about cloud implementation, including those regarding when data can be moved to offshore cloud environments.

In particular, technology, platform, and cloud deployment and service model neutrality should be retained to ensure that the best solutions are adopted. As highlighted in earlier sections, different deployment or service models have different implications for data ownership, responsibilities, and security. No "one size fits all" cloud deployment model or services option will respond best to each ministry's, department's, or agency's widely ranging needs or goals. As such, cloud policies should promote choice and enable government entities to select cloud architectures that are fit for their purposes. In most governments, this approach will likely result in a mix of public, private, hybrid, and traditional on-premises computing models.

17 *Australian Government cloud computing policy version 3.0*. Australian Department of Finance. October 8, 2014. http://apo.org.au/research/australian-government-cloud-computing-policy-version-30

3 Data-aware

PRINCIPLE: Cloud policies should demonstrate data awareness by ensuring that assessments, categorization, and protection of data are commensurate with risk.

Data governance and the processes associated with it have been used for decades to help large organizations and governments manage the integrity of their data. These processes have grown in importance with the advance of cloud computing, as understanding which (and when) data can be shared has become pivotal, especially to fully utilize open data platforms. Governments need to have confidence that their data is appropriately protected from unauthorized access or tampering and that their data is only used in a manner that is consistent with the privacy expectations of their citizens. They need to know that operational disruptions in cloud or network service providers will not adversely affect their ability to function and provide essential services. Moreover, in a dynamic environment of new opportunities and economic imperative, they need confidence that their choice today will not restrict choices that they might need to make tomorrow.

Cloud computing introduces new technical challenges related to what has typically been the domain of information assurance. For example, cloud services are often provided by different CSPs, making direct control over data challenging. Moreover, data hosted in the cloud is never static but moves between services and devices. As a result, CSPs need to ensure that data remains assigned the same value—for example, confidential—whether at rest, in process, or in transit. Additionally, given the global nature of cloud services, data may move across borders.

Cloud providers can only address these issues effectively if governments include, as part of their cloud policies, a conscious approach to data governance. Effective data governance can help to ensure that data stays within the confines of a regional selection that a particular government prefers, for example ensuring that data only travels between countries with data transfer agreements in place. In addition, robust data governance enables government entities to realize optimizations and compliance efficiencies that might not be possible when all data is assigned the same value. Therefore, governments should categorize their data by sensitivity and business impact, considering their relative concerns if data were to be leaked, tampered with, or made unavailable. Below, we introduce two terminology models based on industry-respected models.

Sensitivity	Model 1	Model 2
High	Confidential	Restricted
Medium	For internal use only	Sensitive
Low	Public	Unrestricted

[18]

Any data governance effort should endeavor to understand the needs of the specific, data-owning entity and consider how data is stored, processed, and transmitted throughout the organization. Microsoft therefore recommends that processes for choosing among cloud solutions and for classifying data be developed and implemented within the realm of the ministries or departments themselves, consistent with the "Flexible" principle. Even within a ministry, great variation with regard to data, services, and

18 Simorjay, Frank. *Data classification for cloud readiness.* Microsoft Trustworthy Computing. 2014. http://download.microsoft.com/download/0/A/3/0A3BE969-85C5-4DD2-83B6-366AA71D1FE3/Data-Classification-for-Cloud-Readiness.pdf

constituents exists; a ministry may house groups responsible for military defense or diplomacy in addition to inter-ministerial administrative services, and those entities likely have varying outlooks, not only on how ICT decisions should be approached but also on how their data should be processed and classified.[19] Finally, the way in which an organization classifies its data or service may change over time, so data governance should be regularly revisited to ensure that organizations continually optimize for cost effectiveness and compliance efficiency.

Best practice: UK government optimizing for cloud computing with its data governance[20]

Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss, or misuse) and the need to defend against a broad profile of applicable threats. In 2014, the UK government simplified its system, reducing the number of its security classification levels from six to three. Its information assets may now be classified as one of three types:

- **Official. The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen, or published in the media, but none of which is subject to a heightened threat profile.**
- **Secret. Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors (for example, where compromise could significantly damage military capabilities, international relations, or the investigation of serious organized crime).**
- **Top secret. The government's most sensitive information, which requires the highest levels of protection from the most serious threats (for example, where compromise could cause widespread loss of life or could threaten the security or economic well-being of the country or friendly nations).**

Each level is associated with a baseline set of security controls, providing appropriate protection against typical threats. Additionally, ICT systems and services may require enhanced controls to manage the associated risks to aggregated data or to manage integrity and availability concerns.

In simplifying its security classification system from six levels to three, the UK government found that about 90 percent of its data could be marked "Official." As a result, most of the UK government's data is appropriate for cloud services that can be offered by a wide range of suppliers, incentivizing those CSPs to go through the applicable level of the government's security accreditation processes.

19 *Security Framework for Governmental Clouds.* Op. Cit.

20 "Securing technology at OFFICIAL." UK Government Cabinet Office. March 6, 2015. https://www.gov.uk/government/collections/securing-technology-at-official

4 Risk-based

PRINCIPLE: Cloud policies should prioritize the assessment, management, and reduction of risk in the delivery of cloud services for governments.

Although cloud computing offers numerous potential security and resilience benefits, as with on-premises ICT, it also introduces risks that must be identified and managed. For any system or technology, key early steps in effectively managing risks include identifying, assessing, and prioritizing them. In addition, in introducing cloud computing, government entities should not only identify and assess risks inherent in new systems but also identify and asses those in existing solutions, including in on-premises ICT. In doing so, they can determine both how their risk profile may be improved by migrating to cloud services and what net new risks need to be managed.

During this process, government entities should also strive to distinguish between risks that are likely to be common and risks that are likely to be unique to their contexts or missions. Taking this step eases the later processes of risk management, during which entities must determine how to treat the risks that they have identified, assessed, and prioritized. More specifically, governments and other organizations must decide how to treat risks by determining which they will mitigate, transfer, or accept and by clearly documenting how they plan to do so. As described in the inset, the Security Assurance Framework for Evaluation (SAFE)[21] offers guidance for governments making prioritization and management decisions.

Best practice: Using the Security Assurance Framework for Evaluation to assess, manage, and reduce risk[22]

The Security Assurance Framework for Evaluation (SAFE) is a structured, lightweight methodology for comparative assessment of compliance and risk in relation to modern, cloud-based applications. It is service- and technology-agnostic and consists of five distinct stages, one of which describes how to perform a holistic risk assessment across the assurance domains of trustworthiness (confidentiality, integrity, transparency, privacy, predictability, and exploitability), resilience (preparedness, responsiveness, survivability, durability, availability, and load tolerance), and adaptability (portability, configurability, flexibility, interoperability, suitability, and extensibility), considering impacts of a strategic, operational, compliance, or technical nature. For each data set, service, or system that a government wants to move to the cloud, these assurance objectives should be weighed, recognizing that public or open data often requires lower levels of assurance than secret or restricted data.

Potential risk events, such as a data breach, disruption of service, or loss of encryption keys, can also be categorized according to those assurance domains. Governments should identify and prioritize the most important risks in each of the domains. Within its risk catalogue, SAFE details 50 possible risk events, demonstrating how to answer questions about risk likelihood, impact, exposure, and tolerance, a process that is also consistent with the International Organization for Standardization (ISO) 31000 standards recommendations. SAFE explains that, ultimately, with a catalogue of risk events and an assessment of its risk exposure and tolerance, a government can determine how it should treat risks.

21 Kavanagh, James. *Assuring the Security of Cloud Services.* Microsoft. 2014. http://aka.ms/safehandbook

22 Ibid.

Prioritized risks may be mitigated or transferred by operational or performance requirements, which are generally communicated between ICT providers and customers and are demonstrated through security certifications, audits, or service level agreements (SLAs), a specific form of contract. As the below principle details, requirements should leverage global standards whenever possible. Recognizing that many common risks are mitigated by requirements reflected in global standards, if governments distinguish between their unique and common risks, then they can focus on mitigating, accepting, and documenting their unique risks.

Finally, cloud policies should recognize that risk assessments and management decisions are best implemented as a continual process rather than framed as an end state. As technology evolves and threat actors grow more sophisticated, risk assessments and management decisions must adapt, assessing whether current operational or performance requirements are still sufficient. Additionally, technologies that allow for effective mitigation of previously accepted risks may become available. Due to the dynamic nature of risk, then, risk assessment and management initiatives should be regularly updated as part of an ongoing process.

5 Standards-based

PRINCIPLE: Cloud policies should leverage global standards as the basic requirements for increasing security and resiliency in government cloud services.

To mitigate the risks of any technology, some requirements are essential. A central goal of risk prioritization is not only to focus on areas that are most critical but also to ensure that requirements don't become too broad, all-encompassing, and unwieldy, ultimately making the implementation of secure ICT impossible or impractical and compliance too costly. To increase the practicability and efficiency of developing and implementing requirements and demonstrating compliance, Microsoft recommends that governments leverage global standards to the maximum extent possible. Cloud computing is based on aggregation and scale to drive down costs, so adopting standards used by public and private sector entities around the world will not only reduce the costs of security certifications but also increase the likelihood that more cloud providers are able to demonstrate compliance, resulting in greater market competition.

In 2013, the European Telecommunications Standards Institute (ETSI) reported that many "good" and "sufficiently mature" standards for cloud security already exist and that the cloud standards landscape is large but not as chaotic as it may seem.[23] Indeed, existing global certifications and attestations, including International Organization for Standardization (ISO) 27001 and ISO 27002, ISO 27018, and Service Organization Controls (SOC) 1 and 2,[24] provide most government entities with a reasonable set of security domain coverage for cloud services. Therefore, entirely new requirements and certifications should only be developed when governments require that CSPs take on activities to achieve security outcomes beyond what those cloud providers already achieve with existing audit regimes. If new certifications do not remove the need for existing certifications or address substantial net-new domains, then new certifications will cause marketplace confusion rather than increase security and resilience.

23 *Cloud Standards Coordination: Final Report.* European Telecommunications Standards Institute. November 2013. http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

24 "ISO/IEC 27001 – Information security management." ISO. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm; "ISO/IEC 27018:2014 – Information Technology: Security Techniques: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors." ISO. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498; "SOC 1: Report on Controls at a Service Organization Relevant User Entities' Internal Control over Financial Reporting." American Institute of CPAs (AICPA). http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/aicpasoc1report.aspx; "SOC 2: Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy." AICPA. http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Report.aspx

Best practice: UK re-using cloud certifications to create efficiency and ensure consistency[25]

In the United Kingdom, the G-Cloud framework, which substantially leverages the global standard ISO 27001, and the Digital Marketplace have created a consistent and reusable mechanism for security assessments. Within the G-Cloud framework developed by the UK government, CSPs define the cloud services that they are providing and they specify the level of business impact for which the service is accredited. In addition, the Digital Marketplace allows for UK ministries and departments to search for cloud services that are covered by the G-Cloud framework. Ultimately, the G-Cloud framework and Digital Marketplace ease UK government procurement of cloud services, enabling ministries and departments to utilize sufficiently secure cloud services without going through their own time-consuming and difficult security requirements development and assessment process. Likewise, the G-Cloud system is efficient for CSPs, incentivizing more cloud providers to engage with the UK government. As such, with sufficient confidence and trust in a central certification system, reuse offers significant benefits, including minimizing cost for CSPs and cloud-consuming government agencies and ensuring consistency in the evaluation of security requirements.

While global standards help to optimize for trustworthiness, consistency, and repeatability, governments are not always able to rely upon them; unique requirements may occasionally result from unique risks. However, the cost of unique requirements is relatively higher for cloud services than for on-premises ICT solutions; cloud-based systems are architected to be automated, on-demand, scalable, and continuously updated with enriched feature sets, so excessive one-off, customer-specific requirements can pose substantial challenges to the provisioning of seamless and agile cloud services. In addition, engineering new cloud technologies has led various CSPs to design cloud-based systems differently, which, in turn, has led to variations in how CSPs implement security requirements to address common risks.

Given this inherent variability in design among cloud service offerings, unique requirements need to be adaptable, allowing for various mechanisms or controls to mitigate unique risks and enabling governments to retain their power of choice among various CSPs. Such adaptability must be supported by requirements that are outcome-oriented, developed by governments that focus on what outcome is need, not how best to achieve that outcome. By focusing on outcomes rather than methods, governments permit CSPs to find the most innovative and practical solutions. Outcome-based approaches also ensure that ICT security policies are future-proof and that governments can access technology advancements as they develop. For instance, allowing CSPs to use a range of evidence to demonstrate a wanted government outcome enables CSPs to retain agility, permitting not only for the rapid addition of new services and enriched feature sets but also for CSPs to continue to innovate to better counter existing and emerging security threats, thereby advancing customer security and resilience.

25 "Find people and technology for digital projects in the public sector." UK Government. June 4, 2015. https://www.gov.uk/digital-marketplace

6 Transparent

PRINCIPLE: Cloud policies should establish transparent and trusted processes for developing compliance requirements and for evaluating the security and resiliency of cloud services.

Governments that follow a risk- and global standards-based approach to developing security requirements and addressing resiliency are most likely to adopt cloud technologies effectively. Such an approach can help to guide governments as they assess and understand the contexts in which cloud computing may improve their security. Moreover, it can also help them to ensure that implementation remains cost efficient and practical. However, because cloud computing is a relatively new paradigm and many ministries, departments, and agencies may be procuring cloud services for the first time, implementing a risk- and global standards-based approach may nevertheless be challenging.

As a result, as governments assess their risks and develop requirements, utilizing a process that is open and collaborative is important because it can help to set expectations and avoid misunderstandings. Issues that may need to be addressed differently for cloud services and may therefore emerge as challenging include clarifying the intent of a requirement, reaching consensus on terminology, and determining the technical reasonableness of requirements from the CSP and auditor perspectives. Moreover, cloud introduces between CSPs and their customers a level of shared security and compliance responsibility that should be well articulated and understood from the outset. As such, Microsoft recommends that governments leverage the expertise and perspectives of all relevant stakeholders when developing requirements during a public consultation process, whether through requests for information or a workshop, so that they can establish clear, comprehensive, and easily adoptable compliance frameworks. Implementing an open and transparent requirements development process can also help to preempt unforeseen inefficiencies during the certification or deployment phases.

Best practice: NIST utilizing an open and coordinated process to generate voluntary implementation[26]

In February 2013, the U.S. National Institute of Standards and Technology (NIST) was directed to create a voluntary framework to reduce cyber risks to critical infrastructure. In February 2014, NIST released the first version of its Cybersecurity Framework, which also applies to mitigating cloud computing risks. During its 12-month development of the Framework, NIST ensured that there were many opportunities for industry to provide input. In addition to accepting comments on an initial draft, which was published in July 2013, NIST hosted numerous regional workshops around the United States, inviting global stakeholders to participate in public conversations about what security guidelines the Framework should promote. As a result of NIST's open and coordinated process, U.S. industry understands and is seeking to implement the voluntary Framework. For instance, Microsoft, Intel, and various banks, health care providers, and gas and electric companies have all proactively committed to implementing and benefitting from the Framework.

26 "Cybersecurity Framework." NIST. http://www.nist.gov/cyberframework/

In addition, in evaluating service providers and their security and resilience, Microsoft recommends that governments utilize clear evaluative criteria. More specifically, governments should bring together stakeholders to standardize what constitutes an acceptable substantiation of satisfied security requirements and the sequence of events required by the assessor, delineating the range of deviation allowable from the baseline requirement's recommendations. This is particularly important when the criteria are set for the first time; however, it is also critical that the criteria are regularly revisited to incorporate any new technological solutions, ensuring that governments have the latest security technologies at their disposal.

The importance of transparency cuts both ways, and Microsoft believes that CSPs must be transparent partners with government customers as well. For more than a decade, Microsoft has been committed to trustworthy computing, making sure that our offerings are secure, private, and reliable. In the cloud computing era, we are building on those efforts by advancing our compliance with customer requirements as well as our customers' ability to control security and privacy decisions about their data. We have more certifications and attestations than any other hyper-scale cloud platform provider in the world,[27] and we are focusing on those features that matter most to our customers, such as best-in-class encryption, choice in where data resides, and transparency in how data is handled.

Best practice: Microsoft committing to transparency with government customers[28]

Microsoft has worked to ensure that all of our customers have visibility into our processes, policies, and practices via our Trust Center. Our customers understand and know how their content is managed, what we do to protect data privacy and security, and where their data is stored, accessed, and used.

For governments specifically, we have established the Government Security Program (GSP). The GSP provides national governments with access to important Microsoft product and security resources, including:

- **Source code for key Microsoft products**
- **Transparency Centers to work directly with source code**
- **Vulnerability and threat intelligence from Microsoft**
- **Technical information about Microsoft products and services**
- **A "GSP for Cloud" capability**

27 Keane, Tom. "Microsoft Azure Adds Global Array of New Certifications." Microsoft Azure. June 11, 2015. https://azure.microsoft.com/en-us/blog/microsoft-azure-adds-global-array-of-new-certifications-including-us-dod-disa-level-2/

28 "Government Security Program." Microsoft Trustworthy Computing. http://www.microsoft.com/en-us/twc/government-security-program.aspx

Conclusion

As ICT has evolved, the world has seemingly shrunk and grown more complex. Across trade, human rights, the environment, technology, and many others topics, the process of developing effective policy positions and implementing legislation has become more challenging. Policy makers today must continuously make thoughtful, multi-disciplinary decisions to respond to the challenges of their growing populations, increased interconnectivity, changing expectations of their government services, and the uncertainties of sovereignty in cyberspace. Implementing policy frameworks that enable them to meet those challenges while preserving the core needs of any user—security, resiliency, and performance—is therefore essential.

As such, governments must develop cloud policies and requirements that both create opportunities for innovation and ensure that basic ICT needs can be met. The six principles described in this paper introduce a framework that enables governments to set a clear path toward innovating and advancing their security and resiliency goals. Such a policy can ease coordination, enable peer-based, cross-governmental learning, and perpetuate government goals. To do so, the policy must be broad and adaptable, guiding ministries but not mandating processes or technology decisions that are better determined at the organizational level.

Security and resilience have been identified as prime areas of focus because they have become essential to successful operation of modern governments' ICT systems. Importantly, governments must not wait for a crisis situation to establish their cloud computing strategies and to test their plans for achieving ICT resilience and security. Rather, whether they use public cloud services by default or as a failover option in crises for more sensitive data, governments must be confident that, if a crisis does unfold, the integrity and availability of their data and essential services will remain intact.

In adopting the principles described in this document, governments can take an important first step toward achieving such goals. In addition, governments must develop the requisite resources and skills to undertake data governance processes, assess and determine how best to manage their risks, and meet the operational security and resiliency needs set forth in their national cloud strategies or policies. Such challenges and others will be considered in forthcoming publications.

Microsoft