From Vision to Procurement: Principles for Adopting Cloud Computing in the Public Sector

asia
cloud
computing
association

Acknowledgements

This report was made possible with the support of Microsoft. The ACCA would also like to acknowledge the Members of the Public Sector Special Interest Group (PS SIG) for their contributions:

Jarom Britton, Microsoft (Chair)
Roger Somerville, AWS
Lilian Rogers, AWS
Amanpriet Dhingra, Equinix
Eric Hui, Equinix
Chan Yam Ki, Google
Barbara Navarro, Google
Aruna Withane, Google
Marcus Bartley Johns, Microsoft
Sassoon Grigorian, Salesforce

ACCA Secretariat:
Lim May-Ann, Executive Director
Sarah Lee, Report Production Lead

The ACCA is the apex industry association representing the stakeholders of the cloud and data ecosystem in Asia Pacific. Our mission is to accelerate the adoption of cloud computing in Asia through the creation of a trusted and compelling market environment, supported with a safe and consistent regulatory environment for cloud computing products and services.

The ACCA works to ensure that the interests of the cloud computing and data community are effectively represented in the public policy debate. Drawing on subject-matter expertise from member companies, working groups and special interest groups, the ACCA constantly develops best practice recommendations and other thought leadership materials to achieve our mission. As a vendor-neutral industry association, we welcome engagement with all members and stakeholders in the public policy and government sectors.

To find out more about how to get involved and how to join us as a member, email secretariat@asiacloudcomputing.org, and visit our website at www.asiacloudcomputing.org

Asia Cloud Computing Association

From Vision to Procurement:
Principles for Adopting Cloud Computing in the Public Sector

Table of Contents

Table of Focus Notes

Foreword

One of the most exciting things about the Asia-Pacific region in the 21st century is the sense that opportunities are all around us and that the world is increasingly looking "east" for inspiration to solve the challenges that affect humanity. With many young and diverse populations, fast-growing economies and vibrant, connected communities, there is a feeling of limitless potential.

Nearly every government in the region has concrete, published plans to capture this moment of optimism and possibility to revolutionize their countries. A common feature of all these vision statements, from Japan's *Society 5.0*[1] to the PRC's *Made in China 2025* agenda[2] to Australia's *Digital Transformation Strategy*[3] and the *Digital India* programme,[4] is a recognition of the central role that science and technology needs to play in achieving the desired outcomes.

I frequently meet with government departments and public sector agencies around the region where I am privileged to learn about their ambitions to contribute to their society's development and fulfil their respective government's vision for tomorrow. Too often though, I also hear them expressing dismay that those visions are not realized due to perception issues and operational difficulties in translating them into reality.

Often several unaddressed challenges may be hindering agencies' ability to procure and deploy the next-generation technologies that will make a real difference. Sometimes there is a (real or perceived) lack of clear direction from senior leaders as to the permissibility of new technologies, many of which by necessity must be based on cloud computing services. In cases where senior officials have endorsed "cloud-first" policies, overly cautious, prescriptive, or outdated regulations, even relatively minor provisions of seemingly unrelated rules, can also effectively block adoption.

That is why I am happy that the Asia Cloud Computing Association has taken the step to publish this paper. This booklet reflects the feedback that I and others have consistently heard from multiple governments around the region about what they need cloud service providers to demonstrate in order to drive actual procurement and deployment of cloud computing solutions. I am particularly pleased with the clear, actionable recommendations in each section directed not just to policymakers but also to procurement staff. I believe that by implementing these recommendations and especially *partnering* with potential cloud service providers, public sector agencies will be able to help the digital transformation vision become reality in the Asia-Pacific region.

Jarom Britton
Chair, Public Sector Special Interest Group
Asia Cloud Computing Association

[1] Government of Japan, Cabinet Office, "Society 5.0", https://www8.cao.go.jp/cstp/english/society5_0/index.html.

[2] The State Council, The People's Republic of China, "Made in China 2025", http://english.gov.cn/2016special/madeinchina2025/.

[3] Australian Government, Digital Transformation Agency, "Digital Transformation Agenda", https://www.dta.gov.au/our-projects/strategies/digital-transformation-strategy.

[4] Government of India, Ministry of Electronics & Information Technology, "Digital India", https://www.digitalindia.gov.in/.

Executive Summary

Artificial Intelligence, machine learning, data analytics, the Internet of Things, blockchain, and augmented reality – these are just a few of the truly transformational technologies that have recently emerged. They present an unprecedented opportunity for both the private and public sector to streamline and improve present day processes and services, design new product and service offerings, and create new methodologies and models – all to meet and exceed the expectations of a new generation of consumers.

Governments have encouraged and incentivized the private sector to implement these technologies in their business operations. Governments and public sector agencies are also increasingly seeking to make use of the opportunities and efficiencies that these new technologies offer.

All of these transformative technologies have a common essential enabler underpinning them – they are all powered by cloud computing.

Cloud computing is a scalable, cost-efficient and highly-secure solution to help the public sector transform their services and drive efficiencies. Many governments (including Australia,[5] the Philippines,[6] Singapore,[7] the UK[8] and the US[9]) have adopted "cloud-first" policies for their public sector. These policies encourage, and in some cases mandate, the use of cloud solutions in the public sector. For example, in 2018 the Federal Government of Australia released a Secure Cloud Strategy that requires public agencies to adopt cloud solutions. The message in the Strategy was clear:

> *"The case for cloud is no secret to industry or government. A move to cloud computing – away from on premises owned and operated infrastructure – can generate a faster pace of delivery, continuous improvement cycles and broad access to services. It can reduce the amount of maintenance effort to 'keep the lights on' and refocus that effort into improving service delivery."*[10]

By taking advantage of cloud computing, governments and public agencies can optimize their IT spend, enabling them to better focus their resources where they have unique expertise: governing and administering public programs.[11]

But to effectively enable public sector cloud procurement, discussions need to advance beyond just cost and security. Appropriate procurement processes that provide clear guidance on how cloud can be

[5] Australian Government Cloud Computing Policy, October 2014, at http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf.

[6] The Republic of Philippines Department of Information and Communications Technology, Circular No.2017-002, at http://www.dict.gov.ph/wp-content/uploads/2017/02/Signed_DICT-Circular_2017-002_CloudComp_2017Feb07.pdf.

[7] Infocomm Media Development Authority, 3 November 2017, at https://www.imda.gov.sg/infocomm-and-media-news/buzz-central/2011/7/government-outlines-multipronged-cloud-strategy.

[8] Press Release, UK Cabinet Office, 5 May 2013, at https://www.gov.uk/government/news/government-adopts-cloud-first-policy-for-public-sector-it.

[9] Office of the Federal Chief Information Officer, Federal Cloud Computing Strategy, at https://cloud.cio.gov/strategy/.

[10] Australian Government Digital Transformation Agency, Secure Cloud Strategy, at https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/cloud/secure-cloud-strategy.pdf.

[11] For example, a report by Deloitte found that cloud adoption reduced IT capital expenditure in organizations by an average of 19%. See Deloitte, "Economic and social impacts of Google Cloud", September 2018, at https://www2.deloitte.com/content/dam/Deloitte/es/Documents/tecnologia/Deloitte_ES_tecnologia_economic-and-social-impacts-of-google-cloud.pdf.

procured are also critical. Research by Oracle and the Center for Digital Government[12] reported that government officials felt that they needed a guide to help them through the challenge of buying a service, like cloud computing, that is significantly different than the products and services for which traditional procurement policies and systems are designed. The same report found that only 42% of the respondents had formal cloud procurement methodologies.

The Asia Cloud Computing Association (ACCA) has contributed a significant amount of guidance on procuring cloud services. In 2014 the ACCA published a set of Safe Cloud Principles for the financial services industry.[13] Still, there are certain topics that governments and public agencies must consider when procuring cloud services that are distinct from private sector procurement issues.

The ACCA is delighted to present this white paper to help demystify cloud solutions and provide necessary guidance to procurement policymakers and public sector agencies that are evaluating cloud services.

This paper outlines seven principles distilled from conversations with government procurement officers, policymakers, and auditors where they have told the ACCA and its members what the essential elements are to enabling adoption of technology solutions in the public sector. The discussion is also based on the ACCA's experience reviewing and contributing to cloud computing policies throughout the region. These principles are intended to help policymakers and procuring agencies work in a systematic way through the necessary considerations and have appropriate discussions with potential cloud service providers when:

- developing rules and policies that affect adoption and procurement of cloud computing solutions, including "cloud-first" policies; and
- evaluating the suitability of cloud solutions and cloud service providers for public sector workloads.

Each principle is accompanied by one or more specific, concrete recommendations for policymakers and procuring agencies to follow. By incorporating these recommendations into rules affecting procurement, **policymakers** can provide necessary clarity to procurement officers about the relevant criteria for assessing potential solutions. In the past, lack of clarity has sometimes hampered implementation of announced "cloud-first" strategies. **Procuring agencies** and officers can use the recommendations directed at them to help purchase and deploy cloud services in a more streamlined, efficient way, which will help them to achieve their desired outcomes more fully, quickly, and with less effort.

[12] Understanding Cloud Procurement: A Guide for Government Leaders, at http://www.oracle.com/us/industries/public-sector/understand-cloud-procurement-wp-4423120.pdf. CDG conducted 16 phone interviews in May and June 2017 with 24 state IT and procurement officials and gathered an additional 66 responses from state IT and procurement employees involved with cloud procurement through an online survey fielded in June 2017. In total, CDG collected responses from 82 individuals representing 38 states.

[13] Safe Cloud Principles for the Financial Services Industry, 2014, Asia Cloud Computing Association, at http://www.asiacloudcomputing.org/images/research/2014_-_Safe_Cloud_Principles_for_FSI.pdf.

The seven principles are grouped into three main themes:

1. Protecting Government with the Cloud

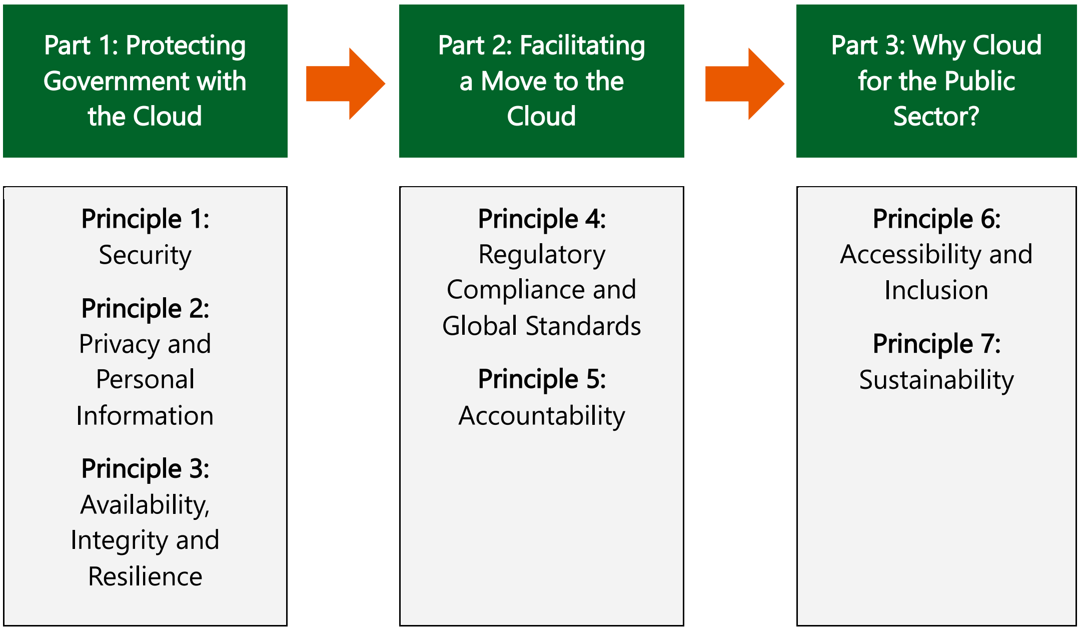
Many organizations, including governments and public agencies, have concerns about the inherent ability of cloud technologies to safeguard their data and operations. These include worries about the security and safety of data stored on the cloud, concerns about handling personal information and complying with privacy laws, and issues with the availability of information stored on the cloud and the ability of cloud solutions to respond to disruptive events. Not addressing these underlying concerns can lead to governments adopting data classification, data localization, data sovereignty, and data segregation rules that prevent cloud adoption but do not actually enhance protections. The principles in this theme explore each of these concerns in detail and demonstrate how cloud solutions actually increase confidentiality, integrity and availability of information and operations compared with traditional on-premises solutions.

2. Facilitating a Move to the Cloud

Government procurement teams often have to grapple with the strategic question of whether applicable mandatory regulations and audit standards (developed for traditional, on-premises IT environments) are compatible with adopting cloud technologies. Accountability, transparency and delivering value for public money is critically important in public sector procurement. The principles under this theme will discuss how aligning local regulations with global compliance standards can improve uptake and efficiencies while ensuring proper accountability of both cloud service providers and public sector users. Procuring cloud technologies is a dynamic process that helps governments to have greater oversight over, and control of their systems, than on-premises solutions.

3. Why Cloud for the Public Sector?

Cloud computing can also help enable digital transformation in the public sector and governments can deploy cloud-based technologies in innovative and agile ways to meet changing stakeholder demands. Understanding from the outset the opportunity that cloud solutions offer can help determine the best procurement approaches to follow. This theme broadens the scope of discussion beyond simple financial cost savings and operational efficiencies in IT departments to show how cloud computing can help public sector organizations achieve their non-financial objectives such as environmental sustainability, improved access to government services, and enhanced citizen inclusion.



Part 1: Protecting Government with the Cloud

Principle 1: Security

Principle 2: Privacy and Personal Information

Principle 3: Availability, Integrity and Resilience

Part 2: Facilitating a Move to the Cloud

Principle 4: Regulatory Compliance and Global Standards

Principle 5: Accountability

Part 3: Why Cloud for the Public Sector?

Principle 6: Accessibility and Inclusion

Principle 7: Sustainability

Part 1: Protecting Government with the Cloud

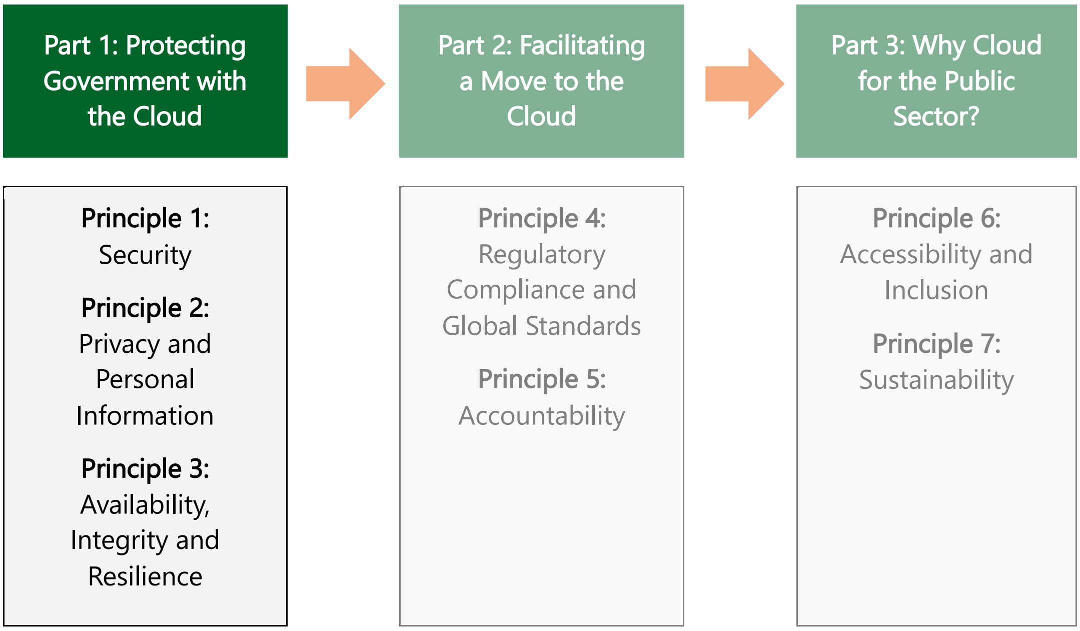
Procurement policies and decisions should be based on accurate, data-driven information. Unfortunately, one of the factors that has sometimes slowed the adoption of cloud-based technologies in the public sector is a (misconceived) cost-benefit analysis: on the one hand, organisations recognize that they stand to achieve significant cost savings by moving their systems to the cloud; but on the other hand, they assume (incorrectly) that this is at the expense of confidentiality, integrity and availability, making the information and systems more vulnerable to attack, disclosure, corruption or breakdown.

In reality, cloud solutions often offer a more protected environment than traditional on-premises systems. This section covers the top three concerns the ACCA hears from public sector agencies related to protection of government data, namely:

1. Security – Security of IT systems is essential for governments and public agencies. Appropriately-deployed cloud solutions can increase an organization's security posture. Separate focus note sections discuss implications for data classification, data localization and data sovereignty, and data segregation policies.

2. Privacy and Personal Information – Governments and public agencies have extensive stores of personal information and need to ensure that information is kept adequately private to maintain the trust of their citizens. Cloud solutions can help governments and public agencies increase the protections and controls over personal information and, in so doing, better comply with applicable privacy laws.

3. Availability, Integrity, and Resilience – Governments need information to be available in real-time, on-demand, and users must be able to trust that the information is reliable. Cloud solutions offer state of the art, purpose-designed infrastructure that reduces the chances of compromises and failures, ensuring that services deployed on the cloud remain available, trustworthy and resilient.



Part 1: Protecting Government with the Cloud

Principle 1: Security

Principle 2: Privacy and Personal Information

Principle 3: Availability, Integrity and Resilience

Part 2: Facilitating a Move to the Cloud

Principle 4: Regulatory Compliance and Global Standards

Principle 5: Accountability

Part 3: Why Cloud for the Public Sector?

Principle 6: Accessibility and Inclusion

Principle 7: Sustainability

Principle 1: Security

Information management systems security is fundamental for the public sector.

There is a persistent belief amongst some people that cloud IT services are not as secure as on-premises IT services. This myth stems from the perception that by having a third party manage your services and information for you, or by putting information on a platform that is accessible remotely via the Internet, security of those systems and information is inherently reduced.

Is my government data safe on the cloud?

The reality, as outlined in the Australian government's Secure Cloud Strategy, is that "cloud [service] providers often implement and manage better IT security controls than internal IT teams as it is a core part of their business and reputation."[14] New Zealand's government also recognizes that "cloud services from global providers are typically more secure than traditional IT systems."[15] Due to their specialization and economies of scale, dedicated cloud service providers, especially hyper-scale ones, can invest vast resources into building some of the most secure physical and virtual infrastructure facilities in the world. Consequently, they often have better technical infrastructure capabilities, risk management practices, detection and suppression systems, incident response and recovery abilities and automated processes than most organizations.

Several features of cloud computing tend to make it more secure than on-premises implementations. For example:

- Data in-transit to, and stored at-rest in, the cloud benefits from high levels of encryption by default.
- Data centres maintained by cloud service providers are highly-secure facilities with multiple levels of physical and logical security and access controls.
- Cloud service providers often have greater resources to update their services with the latest security patches as soon as they become available.
- Cloud service providers implement strong network security protections to detect and respond to potential security threats. Hyper-scale cloud service providers process billions of user authentications every day. This generates extensive information they can draw from to identify potential threats.
- Cloud services often automatically log access and changes to systems and customer environments, generating a tamper-resistant audit trail.

It also is incorrect to assume that a shift to cloud computing is a move away from a secure environment. On-premises environments, which are the main alternatives to cloud services, are familiar but they are in many ways inherently insecure. For example, many of the major recent public sector data breaches

[14] Australian Government Digital Transformation Agency, Secure Cloud Strategy 2017, at https://www.dta.gov.au/files/cloud-strategy/secure-cloud-strategy.pdf.

[15] New Zealand Government, Briefing for Executives: Accelerating Public Cloud: Driving digital transformation, December 2017, at https://www.ict.govt.nz/assets/Accelerating-Public-Cloud/Accelerating-Public-Cloud-Driving-digital-transformation.pdf.

were perpetrated on on-premises systems. The WannaCry ransomware attack that brought down systems of the National Health Service (NHS) in the UK in May 2017 is a case in point. Failure to keep IT systems up-to-date was the primary factor in the success of the WannaCry attack on the NHS.[16] Cloud-based services, which as noted above keep their systems up-to-date, were protected from this attack.

Because of the improved security profile of cloud-based solutions over on-premises infrastructure and applications, the Australian Federal Government's Secure Cloud Strategy requires public agencies to adopt cloud solutions by default. Other governments, including the Philippines,[17] have also recognized the generally superior security profile of cloud-based solutions.

Managing security in the cloud is much like managing security in on-premises data centres, only with greater visibility and auditability of resources, and no need to deal with the costs and complexities of protecting facilities and hardware. Importantly, the cloud enables agencies to formalize account design, automate security and governance controls, and streamline auditing. Instead of relying on auditing security retroactively, the cloud provides security control built-in throughout the IT management process. All this reduces the scope for errors and lapses, thereby increasing the overall security profile.

The ACCA has observed four areas that are especially prevalent and important in government procurement of cloud solutions, and are related to security: data classification, data localization and data sovereignty, data segregation and data privacy. These focus areas are explored further below.

Recommendations

Policymakers should	Procuring Agencies should
1. Expressly recognize the generally greater security offered by cloud-based systems over on-premises systems. 2. Require cloud services' security profile and performance to be assessed using the security profile of the current IT environment as a benchmark.	1. Engage with cloud service providers early in the procurement process to understand how cloud solutions can help keep your systems and data safe and secure. 2. Ensure that tender requirements focus on overall security outcomes rather than prescribing specific security measures that might be incompatible with cloud solutions. 3. Where a cloud solution is at least as secure as your existing environment, do not preclude the solution on security grounds. 4. If your existing environment has been demonstrated to be insufficiently secure, prepare objective, technology-neutral and relevant security criteria *before* measuring all potential solutions – on-premises and cloud – against them.

[16] "Lessons learned review of the WannaCry Ransomware Cyber Attack", Department of Health and Social Care, 1 February 2018, at https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.

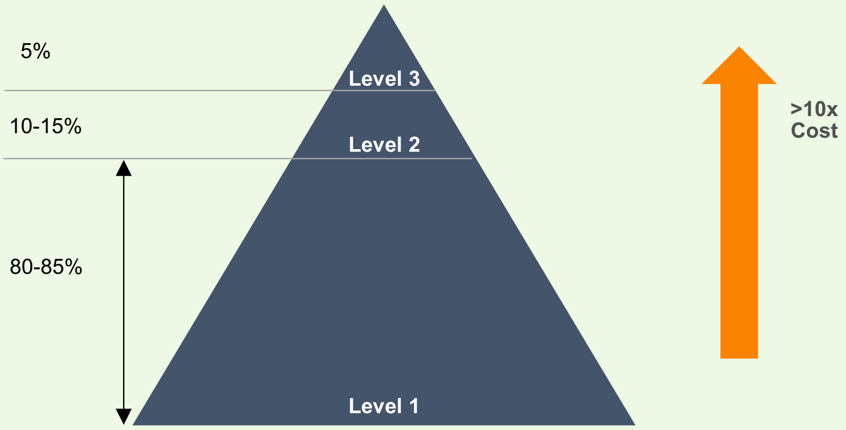
[17] "Prescribing the Philippine Government's Cloud First Policy", Department Circular, Republic of the Philippines, Department of Information and Communications Technology, 18 January 2017, at 5.2.2.

Focus Note 1: Data Classification

Can classified government information be put on the cloud?

Data classification processes group data into distinct ranks based on risk profiles, and then describe the security controls needed at each level to manage risks appropriately. Proper data classification of government data ensures such data is handled based on the potential impact to national security if that data were compromised or lost. Most governments have three or four tiers of classification. For example, Australia employs four security levels (not counting the bottom tier of "unclassified" government data)[18] and the UK utilizes a three-tiered model for government data.[19]

Regardless of the number of classification levels, governments invariably assign most of their data by volume to the lower tiers. Still, for a small percentage of hugely-sensitive data security concerns will outweigh competing considerations. For example, the UK describes 'Top Secret' information as '*exceptionally sensitive HMG (or partner's) information assets that directly support (or threaten) the national security of the UK or allies AND require extremely high assurance of protection from all threats.*'[20] Similarly, the US defines 'Top Secret' data as *'information where unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to national security.'*[21]



Data Sensitivity Levels and Volume

Source: ACCA

Some government departments, like defense ministries, have more highly-classified data as a percentage of their overall data portfolio by volume, but even those departments typically deal with much more mundane data on a day-to-day basis. Many government agencies do not generally have any data that falls into the highest classification tier. Classifying data at the correct level is critical both to national security and the proper and efficient operation of government. Putting cloud computing issues aside for a moment, a major challenge for governments as a whole is the risk of classifying of public sector information at an inappropriate level.

[18] 'Information security management guidelines – Australian Government security classification system', April 2015, Australian Government, Attorney-General's Department, at https://www.protectivesecurity.gov.au/informationsecurity/Documents/INFOSECGuidelinesAustralianGovernmentSecurityClassificationSystem.pdf.

[19] For more information on the approach taken by the UK see 'Government Security Classifications', May 2018, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf.

[20] Ibid. page 9.

[21] Executive Order 12356, Section 1.1(a).

Underclassification of data, or assigning a classification level to information that is too low given the potential impact to national security of a breach, raises the most obvious risk. Lower data classification levels use less-strict security controls, posing risk of that data being compromised.

Because the impact of data underclassification is so salient, officials are sometimes inclined to opt for a higher classification "just to be safe." However, overclassifying data has serious potential implications. Each increased level of classification imposes significantly increased costs to maintain the associated supporting security infrastructure. The UK government in its Government Security Classifications paper[22] specifically stated that applying inappropriately high classification leads to unnecessary and expensive protective controls and reduced information sharing. Recognizing the harm caused by overclassification, the US government mandates that when in doubt officials are to opt for the *lower* classification level for data rather than the higher one.[23]

Just as underclassification threatens national security, security can also be compromised by overclassifying information. A US Congressional hearing examining the costs of overclassification quoted the head of the 9/11 Commission into the 2001 terrorist attacks that too much secrecy had left the US vulnerable: *'Three quarters of what I read that was classified should not have been.'*[24] The same hearing referenced the following paragraph from the 9/11 Commission Report:

> '*No one has to pay the long-term costs of over-classifying information, though these costs – even in literal financial terms – are substantial. There are no punishments for not sharing information. Agencies uphold a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration.*'[25]

This discussion is relevant for procurement teams and cloud services providers in that, typically-speaking, government data at the highest classification tiers is restricted from being stored offshore, or even in some cases off government premises. This often precludes that information from being able to be stored on the cloud. The ACCA does not dispute these policies, but rather emphasizes the importance to governments and citizens of getting the classification right.

Recommendations

Policymakers should	Procuring Agencies should
1. Advocate appropriate data classification according to existing state secrecy laws.	1. Take a risk-based approach to data classification, having considered the risks of impact to national security associated with unauthorised disclosure and access. Classification should not be based on the source or the nature of the information or other criteria. 2. Bear in mind the risks of underclassifying and overclassifying data.

[22] 'Government Security Classifications', May 2018, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf, page 13.

[23] Executive Order 13526 of December 29, 2009, section 1.1(b).

[24] 'Examining the costs of overclassification on transparency and security', Hearing before the Committee on Oversight and Government Reform House of Representatives 7 December 2016, at https://fas.org/sgp/congress/2016/overclass.pdf, page 61 and Cox News Service, July 21, 2004.

[25] Ibid page 77 and 9/11 Commission Report, at https://www.9-11commission.gov/report/911Report.pdf, page 417.

Focus Note 2: Data Localization and Data Sovereignty

Should my government data stay in-country?

Cloud service providers often store data in various locations, either regionally or globally, which improves the functionality, efficiency and reliability of their services. While most countries do *not* have them, some governments impose data localization requirements, which require certain data sets to remain in a particular location or at least within a particular territory.[26]These rules, which are usually developed as or descended from regulations controlling physical documents, are sometimes applied to cloud services even though in the cloud context they do not in fact provide more security.

Data sovereignty is related to data localization but is often confused with it. Data sovereignty is the idea that data is subject to the laws of the legal jurisdiction(s) in which it is collected and stored. Because of this, some public sector agencies fear that data stored in a foreign legal jurisdiction could be more susceptible to seizure than if it remained onshore and so propose data localization rules to try to preserve sole legal authority over the data. In reality, many cloud providers' services include mechanisms that can mitigate concerns about sovereignty of data stored offshore to the point that most, if not all, public sector information can move to the cloud.[27] These mitigating mechanisms can be technical (e.g. encryption, hybrid cloud) and legal (e.g. contractual commitments) in nature.

Security risks to a system environment exist whether it is a third-party cloud solution, or an in-house, on-premises system.[28] Most cybersecurity incidents do not involve attackers having physical access to compromised systems, which makes the physical location of those systems irrelevant, and law enforcement demands for foreign enterprise data (including both private and public sector agencies) are vanishingly rare.[29] In a world where cybersecurity and data breaches are not limited by geographical boundaries, *where* data is physically stored (whether on-premises, off-site, or offshore) is much less important for data security than *how* data is stored.

On balance, data localization rules weaken data security. They give hackers more targets and guide them as to where valuable data sets are kept. By reducing competition, they also reduce incentives to secure infrastructure and limit availability of best-in-class cybersecurity solutions.[30]

There is also a general recognition by global trade and industry bodies that data localization regulations are likely to hinder innovation and economic development. In June 2017, the Asian Development Bank Institute published a Working Paper Series on the Trans-Pacific Partnership Rules for Digital Trade in Asia.[31] In that paper, the ADBI states that data localization regulations *"often come at a cost for businesses because they are forced to locate their data storage centers onshore or use computing facilities onshore –which prevents businesses from making the most cost-effective decision."* The same principle would apply to public sector organizations. There are two independent studies cited in the Working Paper to support this:

- a study by the European Centre for International Political Economy[32] estimates that data localization regulations would result in GDP losses in some countries as follows: 0.2% in Brazil, 1.1% in the People's Republic of China, 0.4% in the EU, 0.1% in India, 0.5% in Indonesia, 0.4% in the Republic of Korea, and up to 1.7% in Vietnam; and

[26] "Cross-Border Data Flows: Where are the barriers, and what do they cost?", Information Technology & Innovation Foundation, 1 May 2017, at https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

[27] In fact, New Zealand's government confirms that "most public cloud services used by agencies are hosted in countries that have no significant jurisdictional risks". (New Zealand Government, Briefing for Executives: Accelerating Public Cloud: Driving digital transformation, December 2017, at https://www.ict.govt.nz/assets/Accelerating-Public-Cloud/Accelerating-Public-Cloud-Driving-digital-transformation.pdf.)

[28] Australian Government Digital Transformation Agency, Secure Cloud Strategy 2017, at https://www.dta.gov.au/files/cloud-strategy/secure-cloud-strategy.pdf.

[29] See for example, AWS's Information Request Reports, at https://aws.amazon.com/compliance/amazon-information-requests/ and Microsoft's Digital Trust Reports, at https://www.microsoft.com/en-us/corporate-responsibility/reports-hub.

[30] Bret Cohen, Britanie Hall, and Charlie Wood "Data Localization Laws And Their Impact on Privacy, Data Security And the Global Economy", American Bar Association, Antitrust Vol. 32 No. 1, Fall 2017, at 107, at https://www.americanbar.org/content/dam/aba/publishing/antitrust_magazine/anti-fall17.pdf. See also Manuel E. Maisog, "Making the Case Against Data Localization in China", International Association of Privacy Professionals, 20 April 2015, at https://iapp.org/news/a/making-the-case-against-data-localization-in-china/.

[31] "Trans-Pacific Partnership Rules for Digital Trade in Asia", ADBI Working Paper Series, June 2017, at https://www.adb.org/sites/default/files/publication/321841/adbi-wp746.pdf.

[32] ECIPE Occasional Paper No. 3/2014, "The Costs of Data Localisation: Friendly Fire on Economic Recovery", at http://ecipe.org/publications/dataloc/.

- a study by Leviathan Security Group[33] estimates that data localization laws in the EU and Brazil would force local companies to pay an additional 30–60% for their computing needs.

In 2016, the United Nations Conference on Trade and Development (UNCTAD) stressed that:

> *"it is important for national data protection laws to avoid (or remove) clear obstacles to trade and innovation … this may involve avoiding or removing data localization requirements that go beyond the basic options for the management of cross-border data transfers."*[34]

UNCTAD further encourages countries to strive to engage with all stakeholders and find the optimal balance between protecting data and allowing competition and innovation to thrive.

Recommendations

Policymakers should	Procuring Agencies should
1. Not require data localization on security grounds.	1. Not introduce data localization requirements on security grounds without first conducting an objective analysis and determining that the extreme sensitivity of the data in question and any security benefits of having data located in a segregated facility clearly outweigh the drawbacks and risks, including security risks, that are associated with data localization. 2. Discuss with cloud service providers what technical, legal, and other measures they have in place, including as it relates to law enforcement and government access, to ensure data remains adequately secured and within your control given that data's sensitivity.

[33] Leviathan Security Group (2015), "Quantifying the Cost of Forced Localisation", at https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

[34] UNCTAD, "Data protection regulations and international data flows: Implications for trade and development", at https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_summary_en.pdf, page 8.

Focus Note 3: Data Segregation

Data segregation relates to the way in which data from one entity is kept separate from other entities' data. Security is compromised if one customer can access other customers' data without authorization. There are two primary ways to ensure data is kept separate, or segregated: physical and logical segregation.

Physical segregation exists where data storage and processing infrastructure, such as data centers or server racks, are unique to a particular user or account (known as "tenants"). In physically segregated (also sometimes known as "dedicated") environments, just one tenant's data is kept on a particular server or in a particular data center. If that tenant does not have sufficient data to fill the server or the data center, then that infrastructure sits idle and cannot be used by other tenants. Physically-segregated environments have higher cost structures and limited redundancy options, defeating some of the main benefits to multi-tenanted (or "public") cloud services, and do not provide much in the way of added security or access control compared with logically-segregated systems.

Is my government data at risk in a data center that processes and stores other customers' data?

Best-in-class procurement requirements and controls recognise that multi-tenant[35] environments can typically achieve equivalent security outcomes to physically-segregated ones through logical segregation. Logical segregation uses software controls to keep each tenant's data isolated while sharing the same physical servers as other tenants.[36] Users are granted access only to their data and are not even aware that another tenant's data may be stored or processed on the same equipment, let alone whose data that could be. Data from one tenant is completely isolated from, and cannot influence, data from other tenants that share its physical environment. At the same time, physical infrastructure efficiency is optimized by reducing the amount of idle computing capacity, thereby lowering operating costs.

The US Department of Defense Cloud Computing Security Requirements Guide has acknowledged the use of logical segregation as a viable approach to meet the Department of Defense Impact Level 5 separation requirements (these guidelines otherwise require that the particular type of controlled information covered be processed in a dedicated infrastructure).[37] The Australian Signals Directorate also recognizes logical segregation as being appropriate for most network architectures and advocates implementing physical segregation in addition to logical segregation only as an exception for "particularly sensitive" environments.[38]

Recommendation

Policymakers should
1. Recognize physical segregation and logical segregation as equally secure. Only for extremely sensitive data where security concerns overwhelm all other considerations should physical data segregation be required in addition to, not in place of, logical segregation.

[35] Where multiple customers, or tenants, share the same physical infrastructure, similar to how multiple different companies can be tenants in the same office tower.

[36] 'Security implications of logical separation in the cloud', Microsoft policy papers, at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REXpGk.

[37] 'Logical Separation: An evaluation of the U.S. Department of Defense Cloud Security Requirements for Sensitive Workloads', May 2018, Amazon Web Services Government Handbook Series, at https://d1.awsstatic.com/whitepapers/compliance/AWS_Logical_Separation_Handbook.pdf.

[38] Australian Signals Directorate, "ACSC Protect: Implementing Network Segmentation and Segregation", January 2019, at https://www.acsc.gov.au/publications/protect/network_segmentation_segregation.htm.

Focus Note 4: Privacy and Security – Similar, But Different

It is important for governments and public agencies to appreciate that privacy and security are two separate concepts that should be delineated clearly, especially in the public sector where security aims are different from privacy ones.

Personal data is unquestionably sensitive; health, tax, and criminal records are particularly so. If it is leaked, personal data can cause embarrassment or economic or reputational damage to an individual. But, except for the personal data of some top government officials, personal data leaks do not have implications for national security, nor are they typically considered disclosures of state secrets.

How can we regulate personal data on the cloud?

Classified information and state secrets are on the other hand synonymous. Unauthorized disclosure of classified information can be a treasonous offence under official secrets or espionage laws and carries severe criminal penalties.

Because of this, security and privacy laws have different objectives. The goal of state secrecy laws is to prevent unauthorized disclosure of classified information. Privacy laws instead seek to preserve the ability of individuals to control access, use and disclosure of their personal information.

Privacy regimes often achieve their objective in large part through the principle of notice and consent.[39] Under these regimes, a collector of personal data must notify the individual why their information is being collected and how it will be used and obtain consent from the person to use his or her information in that way. Any use or disclosure of data with the individual's consent is an authorized disclosure or use. The consent is required because the individual is typically the ultimate, permanent owner of the information under the law.

Governments recognize their duty to protect the personal information that has been entrusted to them by their citizens. They also recognize that this information is of varying degrees of sometimes quite-high sensitivity. Some governments have looked to the state security laws, with their ready-made data classification levels, as a means to protect the personal data in their care. The rationale is that because personal information is sensitive, it needs to be protected. Official secrets laws are designed to protect information. Therefore, they argue, it is appropriate to use these laws and policies to protect personal data in their care, which necessitates classifying the personal data

The problem with this logic is that, while it seems like a convenient solution, it conflates security and privacy and confuses the ownership of the data. State secrecy laws were designed to protect government information that, if disclosed, would put national security at risk.[40] As discussed above, classified information is subject to restrictive and increasingly onerous security controls, must be disclosed only to people with appropriate security clearances, carries severe penalties for disclosure to other persons and, in some extreme cases, must be kept onshore. Consent is not a cure-all.

If personal data is subject to state secrecy classifications, contradictions arise when individuals disclose their personal information to multiple parties, many of whom do not have security clearance. For example, citizens will disclose salary information to the government when they pay their taxes but also give it to their bank when they apply for a loan. They will disclose their name and address to apply for a driving license but also to join a retailer loyalty program. None of these disclosures are treated as disclosures of classified information.

Data localization requirements for personal data under state security laws or otherwise also do not work. People have a habit of moving across borders and when they do, they take their personal information with them. They provide it to buy plane tickets, check into a hotel, get a visa, seek medical treatment, pay for meals and entertainment and a host of other things. In each case, they consent to this information being given.

Further, preventing cross-border flows of personal information, even when people consent, can harm people. For example, if health information must not leave a patient's home country, and that person falls ill overseas and requires emergency treatment, inability to access the person's medical history, including

[39] An exception to this rule would be Australia, which generally only requires notice be given by the data collector.

[40] See Bartlett, G. and Everett, M. "The Official Secrets Acts and Official Secrecy." Briefing Paper number CBP07422, UK House of Commons Library, 2 May 2017, at https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7422.

known prior conditions, allergies, etc., can have grave consequences and at the very least, unnecessarily delays treatment.

Finally, classifying personal information under state secrecy laws instead of privacy laws can prevent adoption of cloud computing solutions that could otherwise be deployed to help improve citizen services. For example, this can happen when the assigned classifications mandate data localization.

The good news is that governments have another legislative option that respects the need to keep personal information confidential and at the same time allows citizens to remain in control of that data, ensure its integrity and grant access to it as they choose. Privacy laws are typically designed for precisely this purpose. They recognize that personal information is owned by the individual and not the data collector. They allow the individuals to remain in control of who has access to their data and for what reason. They require data custodians to take steps to make sure that the information is protected from unauthorized disclosure. Data custodians can be held accountable to both individuals and regulators to ensure that they adhere to the standards in the laws.

For all these reasons, governments should use privacy laws to regulate personal information, not state secrecy laws.

Recommendations

Policymakers should
1. Carefully distinguish between security and privacy considerations. 2. Not introduce data localization requirements on privacy grounds.

Principle 2: Privacy and Personal Information

Governments need to ensure that privacy rights are respected.

Does cloud protect privacy?

Personal data breaches now seem almost routine. While many currently go unreported, large-scale breaches at Equifax,[41] Marriott,[42] Singapore's SingHealth[43] and others have made headlines around the world. The increase of social media and an accompanying perceived loss of control over one's online identity and privacy have also caused concern. Cloud service providers therefore need to be able to demonstrate to their government customers and the public how personal data entrusted with them is at least as protected as it is in the hands of the agency that initially collected the data.

Lawmakers are also re-examining how personal information is managed, and the transparency that personal data custodians give to the owners of that information. A new generation of privacy laws, including the EU's General Data Protection Regulation (GDPR),[44] are underpinned by principles of notice, consent, integrity and confidentiality, and prescribe requirements in relation to how personal data should be collected, used, disclosed and processed. The importance of transparency is also emphasized, so that individuals understand how their personal data is being processed. The GDPR currently sets the highest standard for privacy protection worldwide but is similar in many of these respects to data protection regimes in the Asia-Pacific region, including those in Australia, Hong Kong, Malaysia, and Singapore. For example, both the GDPR and Australia's Privacy Act require data to be processed in a "transparent" way, personal information to be kept accurate, individuals to have the right to access their information and individuals to be notified of breaches.

The increased size[45] and frequency[46] of personal data breaches in this decade has coincided with the transformation of IT systems from traditional on-premises to cloud infrastructure. But it would be wrong to draw a causal link between these two developments. While incidents such as the Cambridge Analytica/Facebook scandal[47] have demonstrated the importance of vetting a cloud service provider's privacy policies and procedures, many of the largest and most damaging public sector personal data breaches in recent years, from the Philippines Election Commission (70 million records compromised)[48] to the Turkish citizenship database (50 million records)[49] to the U.S. Office of Personnel Management (21.5 million records)[50] were the result of mishandled personal data and insufficient controls on on-premises systems, not issues with cloud services.

[41] Federal Trade Commission, The Equifax data breach, at https://www.ftc.gov/equifax-data-breach.

[42] Federal Trade Commission, The Marriott data breach, at https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach.

[43] Government Singapore, SingHealth cyberattack: What you need to know, at https://www.gov.sg/news/content/channel-newsasia---singhealth-cyberattack-what-you-need-to-know.

[44] EU's General Data Protection Regulation can be accessed at https://gdpr-info.eu/.

[45] Weise, E., "USA TODAY's list of the biggest data breaches and hacks of all time," USA TODAY, 4 December 2018, at https://www.usatoday.com/story/tech/2017/10/03/biggest-data-breaches-and-hacks-all-time/729294001/.

[46] Privacy Rights Clearinghouse, "Chronology of Data Breaches", at https://www.privacyrights.org/data-breaches.

[47] "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far", The New York Times, 4 April 2018, at https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[48] "Philippines elections hack 'leaks voter data'", BBC, 11 April 2016, at https://www.bbc.com/news/technology-36013713.

[49] "Turkish authorities 'probing huge ID data leak'", BBC, 6 April 2016, at https://www.bbc.com/news/technology-35978216.

[50] OPM, Cybersecurity Resource Center: Cybersecurity Incidents, at https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

Still, as custodians of some of the largest collections of personal data, including very sensitive personal data, governments and public sector agencies recognize the responsibility that they have to ensure that the personal data is not misused and understand that the public trust in them relies in part on their ability to live up to citizens' privacy expectations.

Consequently, any public sector agency's evaluation of a cloud computing solution should include an assessment of the cloud service provider's privacy policies and the measures it takes to maintain the confidentiality of personal data. Further, a move to the cloud should not weaken the control that the public sector agency has over the personal data in its care. Governments should be able to continue to monitor and control access to the data. Cloud service providers should clearly describe the situations in which data may be used or disclosed in their contracts and be able to demonstrate that they have implemented sufficient measures to ensure that personal data is used only in ways that are consistent with their contractual commitments.

Fortunately, many cloud service providers have sophisticated privacy practices and controls and extend data use commitments to their customers. For example, most hyper-scale cloud service providers have committed to GDPR compliance for their cloud services and provide GDPR-related assurances in their contractual commitments to their customers. Some features of modern cloud services actually can prevent inadvertent and intentional data leaks and provide deeper monitoring and control features compared to on-premises systems. Users of cloud services can choose from sophisticated tools to protect personal data, including encryption tools.

Most major data protection laws, including GDPR, permit an organization to transfer personal data overseas – even without the individual's consent – if they ensure that the data is no less protected overseas than it is in its country of origin.[51] It would make sense then that governments contemplating using the cloud to store or process personal data would require a cloud service provider to demonstrate security and technical measures sufficient to ensure at least a comparable level of protection as what they provide for that data on-premises.

Recommendations

Policymakers should	Procuring Agencies should
1. Require appropriate due diligence into privacy practices and policies of cloud service providers to ensure that personal data is no less protected with the cloud service provider than it is with the collecting agency.	1. Have open discussions with cloud service providers about privacy practices and how moving to the cloud can help enhance personal data protection and control over government information systems.

[51] Data transfers to third countries are covered in Articles 44 and following of the GDPR. See also for example Section 26(1) of Singapore's Personal Data Protection Act 2012 and Section 129 of Malaysia's Personal Data Protection Act 2010.

Principle 3: Availability, Integrity and Resilience

Governments need information and technology to be reliable.

Can I trust the cloud to not lose my data?

People today expect IT systems to work and for services to be **available** on-demand at all times. They have little patience for downtime due to system maintenance or upgrading. Governments also rely on official portals and websites to disseminate information and conduct routine transactions that previously required ranks of call center employees and other service personnel. In the past two decades, e-government services have greatly improved access to government and become a crucial factor in citizens' opinion of public administration. Because of this, when IT systems are not reliably available, quality of citizen services and government functions suffers, costs increase and satisfaction plummets.

All organizations need to be able to trust the data that they use. For governments, important decisions that affect the proper functioning of public services, future planning and real-time citizen well-being depends on data being up-to-date and accurate. Ensuring data **integrity** requires not only robust security protocols, but also the ability to verify the data being used.

In the public sector, availability and integrity take on even greater importance in that many of the events that can give rise to widespread system failures (e.g. national disasters, power outages, cyberattacks, etc.) are precisely the times when those systems need to be able to be called upon by authorities to help them restore order, calm citizens, and respond to emergencies. No system is completely fail-proof, but **resilience** – the ability for systems to be restored quickly and to mitigate the risk of data loss and corruption – is essential.

One example of the importance and connectedness of these concepts is in electronic voting systems, which are becoming more common. These systems need to guarantee availability to ensure that ballots can be cast without any downtime during voting hours, integrity to prevent multiple voting, illegal voting and other ballot tampering and resilience to allow the system to cope with and recover quickly from disruption. E-voting systems that do not safeguard these factors fail to maintain the public's trust in the electoral process and the accuracy of election results, which in turn can cast doubt on a government's legitimacy.[52]

Governments and public agencies sometimes think that information becomes less reliable once it leaves the physical and geographical boundaries of the country or even their data center. That is a myth. The fact that information placed on the cloud has left the geographical perimeter of a government's data center or country does not mean that the government or public agency has any less control over, or access to, that data. In fact, evidence from private sector customers about moving to cloud solutions shows exactly the opposite. A cloud trust study commissioned by Microsoft Trustworthy Computing

[52] See e.g. "Indian election 2019: Are fears of a mass hack credible?", BBC, 25 January 2019, at https://www.bbc.com/news/world-asia-india-46987319.

found that 75% of small and midsize businesses said they experienced improved service availability after moving to the cloud compared with just prior to migrating.[53]

As with security, data does not become inherently more or less reliable simply because of *where* that data is stored. Rather, reliability is more a function of *how* the data and infrastructure are managed. Because of the economies of scale and specialization of hyper-scale cloud services, data stored on the cloud can be more reliably-available and data integrity can be preserved better than data stored on an on-premises infrastructure. The geo-diversification of data in the cloud is actually a feature designed to protect it from the types of incidents, such as natural and man-made disasters, that negatively impact availability and resilience of data on on-premises systems.

Cloud solutions offer state of the art, purpose-designed infrastructure that reduces the chances of compromise and failure, ensuring that services deployed on the cloud remain available, accurate and resilient. They offer multiple layers of redundancy, high levels of automation and round-the-clock monitoring. Most cloud service providers offer significant uptime service levels (e.g. of at least 99.5%)[54] in relation to their service offerings.

To preserve data integrity, public sector agencies using cloud solutions can implement sophisticated audit logs that monitor access and changes to data. Further, they can easily create and store multiple redundant and backup copies of data to reduce the risk that it becomes corrupted or lost.

The ability of cloud solutions to respond automatically to changes in circumstances also means that there is a lower likelihood of end-users experiencing system downtime due to extrinsic physical / infrastructural issues such as power failures, natural disasters and sudden surges in demand.

Recommendations

Policymakers should	Procuring Agencies should
1. Require adequate due diligence of cloud service providers' availability statistics and infrastructure, integrity and verification tools, and service level agreements. 2. Require performance benchmarks to be set against existing systems.	1. Have open discussions with cloud service providers about infrastructure, integrity and verification tools, service availability and other available means of ensuring that cloud solutions provide the same or greater availability, integrity and resilience compared to self-managed, on-premises systems.

[53] 'Cloud Security, Privacy and Reliability Trends Study: A Silver Lining in Services Adoption', June 2013, Microsoft Secure, at https://cloudblogs.microsoft.com/microsoftsecure/2013/06/11/cloud-security-privacy-and-reliability-trends-study-a-silver-lining-in-services-adoption/.

[54] See e.g.:
Amazon Compute Service Level Agreement, last updated February 2018, at https://aws.amazon.com/compute/sla/,
Google Cloud Storage SLA", last updated October 2018, at https://cloud.google.com/storage/sla and
Microsoft Online Services SLA, last updated December 2018, available at https://www.microsoftvolumelicensing.com.

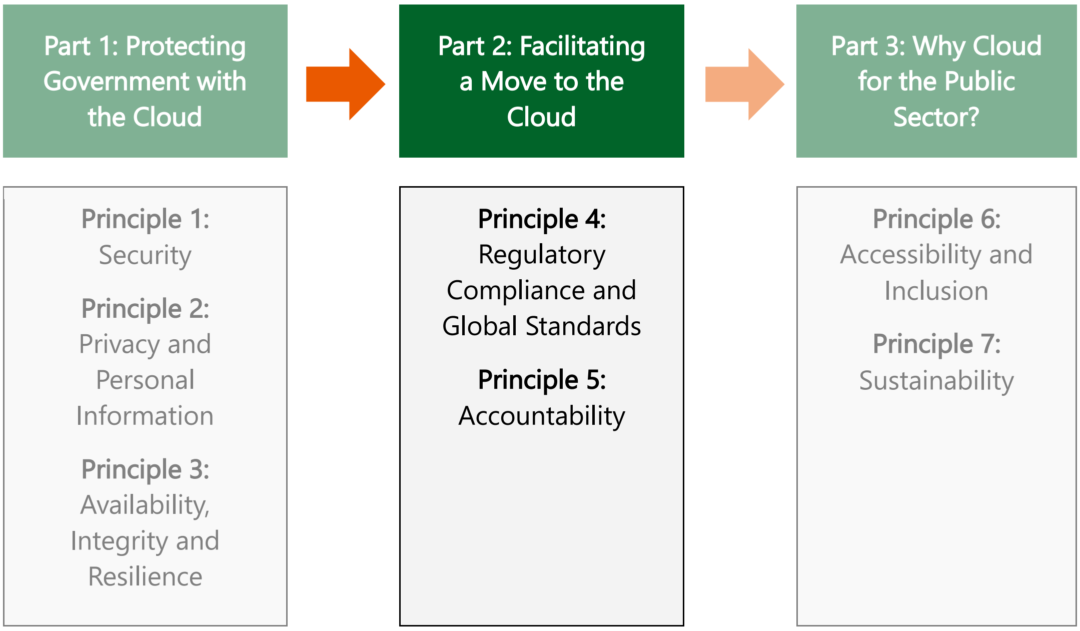
Part 2: Facilitating a Move to the Cloud

Governments need to acquire products and services that are fit for purpose and deliver value for public money. In addition to understanding the benefits that cloud services can provide, public sector customers must also understand how they can enable procurement of cloud services in a way that respects the duties of transparency and accountability that governments owe to their citizens. To do this effectively, they will need to consider what the government's or public agency's compliance requirements are, what standards should be expected of the cloud service provider, and how these agencies must answer to government oversight committees and the public.

This section explores two principles that government policymakers and procurement teams should bear in mind when developing cloud procurement policies and contemplating a move to the cloud:

1. Regulatory Compliance and Global Standards – Cloud services must be measured to clear, verifiable benchmarks for quality and reliability of service. By adopting international standards rather than preparing custom requirements, governments can accommodate their need to verify compliance with performance standards while at the same time enable cloud service providers to preserve one of cloud computing's major advantages – the ability to deliver the same computing services to multiple customers simultaneously.

2. Accountability – Cloud service providers can help governments and public agencies with their accountability and transparency responsibilities toward government oversight bodies and the public. These responsibilities are particularly important in the context of public procurement, where public funds are being used.



Part 1: Protecting Government with the Cloud

Principle 1: Security

Principle 2: Privacy and Personal Information

Principle 3: Availability, Integrity and Resilience

Part 2: Facilitating a Move to the Cloud

Principle 4: Regulatory Compliance and Global Standards

Principle 5: Accountability

Part 3: Why Cloud for the Public Sector?

Principle 6: Accessibility and Inclusion

Principle 7: Sustainability

Principle 4: Regulatory Compliance and Global Standards

Technology solutions must be measured to clear, verifiable benchmarks for quality and service reliability.

How can I assess and protect my interests on the cloud?

Cloud service providers generate efficiencies in large part by offering commoditised IT services on a vast scale to millions of customers. This allows them to invest in industry-leading security and technology at a lower unit cost than any individual customer could. This also means that cloud infrastructure and processes cannot be customised for individual customers without significantly reducing those efficiencies or compromising functionality. Still, public sector agencies need to be able to perform necessary due diligence to ensure that the cloud provider's services offer equivalent or greater overall regulatory compliance to applicable regulations than on-premises alternatives.

A significant benefit of using cloud services is that users can rely on independent certifications of cloud service providers' security and compliance controls to satisfy their regulatory due diligence needs. The independent, non-government International Organization for Standardization (ISO) has published standards relevant to cloud services. Many cloud service providers choose to demonstrate their compliance with international standards by appointing accredited auditors to audit them against these standards and issue a certification. For public sector cloud users, ISO 27001 (information security), ISO 27017 (cloud security) and ISO 27018 (cloud privacy) may be the most useful ISO standards. Many cloud service providers' compliance portfolios go well beyond these standards. By providing ISO certifications, cloud service providers are demonstrating that they have undergone extensive reviews by an external, accredited entity, who has validated that they comply with the controls in the relevant standards.

International standards are a useful resource for public sector agencies when determining minimum standards they should insist on, particularly where the international standard is widely recognized or adopted by other governments. By recognizing equivalence where appropriate, governments can reduce the compliance burden on service providers who do not need to re-certify the same controls. They can also streamline due diligence aspects of their procurement processes and provide assurance to the public that they are adopting international best practice. Developing and maintaining customized standards is also burdensome and expensive for governments and regulators. Creating a new standard takes a significant amount of staff time and hiring consultants with relevant expertise. Once the standard is announced, auditors must be trained and accredited to the new standard. Ongoing monitoring is necessary to ensure that the standard stays relevant and up to date. This is not necessary when governments leverage existing standards.

Another benefit of adopting appropriate international standards is that it avoids the need for duplicative audits. When cloud service providers are certified to a relevant standard, public sector agencies will not need to carry out their own audits, thereby reducing overhead both for them and the provider. Permitting customers to perform their own audits of cloud services is also challenging for providers. With millions of customers, if every customer separately requests evidence of security and operational controls, cloud service providers would quickly be overrun with requests for audits, requiring them to hire new staff to handle those requests. Letting one customer's auditor into a data center could also put other customers' data at risk. Instead, it is more efficient for all parties to have the cloud service provider arrange independent third-party audits for all their customers collectively against each applicable standard and then to make their certifications available to customers.[55]

The Government of Canada provides one example of adopting international standards in this area. Rather than requiring separate certification against its own security guidelines/standards, the Government of Canada published the Government of Canada Security Control Profile for Cloud-based GC IT Services,[56] which cross-references its own standards with prevalent industry certifications, such as ISO 27001. Other frameworks that governments worldwide have adopted are the NIST Cybersecurity Framework[57] and the UK NCSC Cloud Security Principles.[58]

Regulatory compliance challenges can also arise when procurement rules dictate the form of cloud service contracts. Many governments maintain their own standard IT or procurement contracts and require their agencies to use those templates, although those templates are not designed for cloud. Cloud services often allow extensive configuration by the end-user but, unlike other consultancy and outsourcing arrangements, involve the service provider making the same service available to all users without customization by the service provider. If governments insist on using their own standardized terms, they might limit the cloud service providers who are able to contract with them or the services that are available. For these reasons, it is generally more efficient and practical to use the cloud service provider's standard terms as a starting point instead of government-drafted contracts.

Recommendations

Policymakers should	Procuring Agencies should
1. Encourage adoption of applicable international standards rather than creation of unique requirements at the national or agency level. 2. Permit and encourage contracting using the cloud service provider's standard contracts.	1. Require cloud service providers to provide evidence that they hold appropriate certifications and do not request audit rights to check measures that are covered by those certifications.

[55] Audit reports of several major cloud service providers are available from the following sites:
AWS: https://aws.amazon.com/compliance/programs/
Google: https://cloud.google.com/security/compliance/#/
Microsoft: https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide
Salesforce: https://trust.salesforce.com/en/compliance/.
Some providers also make more detailed reports available to customers under non-disclosure agreements.

[56] 'Government of Canada Security Control Profile for Cloud-based GC Services', March 2018, Government of Canada, at https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html.

[57] 'Cybersecurity Framework', National Institute of Standards and Technology, U.S. Department of Commerce, at https://www.nist.gov/cyberframework.

[58] 'Implementing the Cloud Security Principles', National Cyber Security Center, Government Communications Headquarters, 21 September 2016, at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles.

Principle 5: Accountability

Technology procurement must align to agencies' duty of accountability.

How can I demonstrate transparency on the cloud?

Public sector agencies have stewardship over the public purse. Therefore, they are accountable for properly managing the funds that are entrusted to them. They are subject to oversight and audit from state auditors, comptrollers and auditors general, known generally as supreme audit institutions. Supreme audit institutions are increasingly responsible not just to conduct financial and compliance audits, but also to make recommendations on the reliability, effectiveness, efficiency and economy of government programs and operations.[59] Any purchase and deployment of cloud services needs therefore to facilitate agencies' transparency and accountability to supreme audit institutions in financial administration and information management.

When it comes to managing expenditures, cloud solutions that are properly deployed and monitored can offer a more efficient use of public funds than on-premises infrastructure by reducing waste and taking advantage of economies of scale. Cloud solutions are often priced based on consumption, which allows users to pay only for what they use, and their shared supporting infrastructure promotes greater efficiency. This eliminates waste and provides for a more economical use of public funds.

Achieving the substantial potential efficiencies and economies of cloud computing requires thoughtful and careful planning and appropriate due diligence. It requires open discussions with cloud service providers to agree on the relevant performance metrics and how they can be measured. Successful adoption of cloud computing solutions implicates a shared responsibility of both the government agency and the cloud service provider so these planning exercises help level-set on each party's respective commitments and accountabilities. Establishing this clarity will aid government agencies to respond to requests from, and be appropriately accountable to, their oversight functions and audit officials.

As part of this discussion with cloud service providers, Australia's Secure Cloud Strategy encourages public agencies to ensure that good information management is implemented in service contracts. Some of the contract provisions and information that the Australian Federal Government recommends discussing with their cloud service providers include understanding the format in which data is stored and where to obtain audit logs.[60] In that is an implicit recognition that cloud service providers are able to help their public sector customers meet their record keeping and transparency requirements. The Secure Cloud Strategy also recognizes that cloud services are "well suited for a streamlined procurement pathway" that achieves efficiencies by speeding up acquisition and deployment of IT services.[61]

[59] OECD, "External Audit – Supreme Audit Institutions', at http://www.oecd.org/gov/external-audit-supreme-audit-institutions.htm.

[60] Australian Government Digital Transformation Agency, Secure Cloud Strategy, at https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/cloud/secure-cloud-strategy.pdf, at 3.4.3.

[61] Australian Government Digital Transformation Agency, Secure Cloud Strategy, at https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/cloud/secure-cloud-strategy.pdf, at 3.2.2.

Many cloud service providers make extensive disclosures about their services' security, privacy and compliance profiles.[62] For example, Amazon Web Services provides customers a wide range of information on its IT control environment through white papers, reports, certifications, and other third-party attestations.[63] Google Cloud publishes its certifications and assessments for its products and shares reports with its customers.[64] Microsoft also shares reports of independent assessments that examine its specific services with its customers.[65] It also makes available to customers information that it provides to auditors and regulators as part of various third-party audits of Microsoft's cloud services.[66] The high level of transparency of these and other cloud service providers is helpful in assisting government agencies with their own audit compliance by helping them understand the controls in place for those services and how those controls are validated.

Cloud service providers also offer enhanced reporting and monitoring capabilities compared with traditional on-premises systems. These capabilities allow users to better track performance and effectiveness of IT systems and measure the quality of service delivery. They provide written service level agreements and tools to monitor compliance with commitments.

Cloud computing services do not involve a one-off sale-purchase transaction. In the most successful cloud deployments, the cloud service provider and local resellers and systems integrators play active roles in IT planning and in providing information necessary to enable the organization and its oversight bodies to evaluate the service and monitor operations on a continuing basis. Supreme audit institutions are valuable independent organizations that can help support cloud adoption by recommending appropriate measures to monitor adoption and deployment.

Recommendations

Policymakers should	Procuring Agencies should
1. Recognize and allow that any major IT restructuring project will be dynamic and that there will be learnings along the way and as technology and needs change.	1. Conduct comprehensive IT planning internally and consult early and on an ongoing basis with compliance departments, supreme audit institutions and cloud service providers to develop your overall cloud computing strategy. 2. Update performance indicators as necessary in consultation with the stakeholders mentioned above.

[62] See e.g. AWS Cloud Compliance website at https://aws.amazon.com/compliance/, Google Trust & Security website at https://cloud.google.com/security/, and Microsoft Trust Center at https://www.microsoft.com/en-us/trustcenter.

[63] See e.g. Amazon Web Services: Risk and Compliance Whitepaper, May 2017, at https://d1.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf.

[64] Standards, regulations & certifications, at https://cloud.google.com/security/compliance/.

[65] 'Achieving trust and compliance in the cloud', Microsoft, at https://aka.ms/cloud-trust-compliance.

[66] 'Audit Reports, Resources to help information security and compliance professionals understand cloud features, and to verify technical compliance and control compliance', at https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_SOC%20%2F%20SSAE%2016%20Reports.

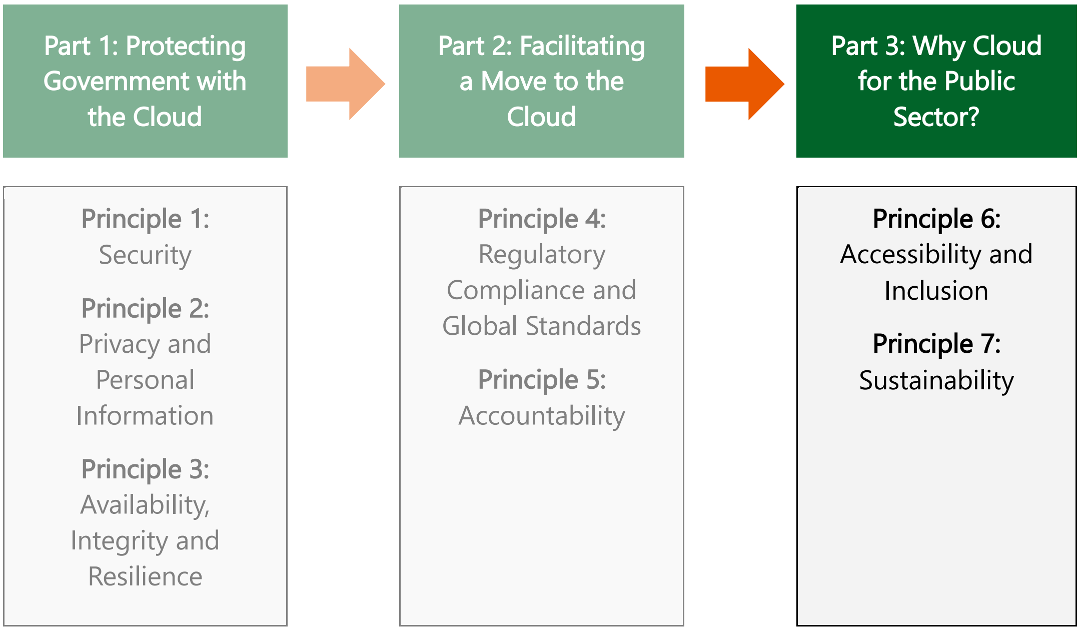
Part 3: Why Cloud for the Public Sector?

The protections offered by the technical architecture of the cloud and the efficiencies associated with cloud services are only the beginning of the benefits that governments and society can realize by deploying cloud-based technologies. The transformational technologies of today are largely powered by cloud solutions. Policymakers and procurement officers should not limit themselves to thinking about the change cloud computing enables within IT departments or the budgetary savings that can result from migrating to the cloud, but should expect cloud-based technologies to offer solutions that enable governments to achieve their broader objectives as well. Agencies that focus only on migrating existing workloads to the cloud or take too narrow a view of cost savings will miss these transformational benefits.

This section discusses two fundamental principles that demonstrate how the opportunities offered by the cloud go beyond security, legal and financial considerations. Procurement policies should encourage procuring agencies to consider how cloud technologies can help achieve objectives in these and other areas:

1. Accessibility and Inclusion – Adoption of technology in general, and cloud computing in particular, should be viewed in light of broader development goals of extending services to citizens and helping people participate more fully in society.

2. Sustainability – Cloud computing can play a role to help organizations reduce their energy consumption and carbon emissions, thereby meeting international commitments for environmental stewardship.


Part 1: Protecting Government with the Cloud
Part 2: Facilitating a Move to the Cloud
Part 3: Why Cloud for the Public Sector?
Principle 1: Security
Principle 2: Privacy and Personal Information
Principle 3: Availability, Integrity and Resilience
Principle 4: Regulatory Compliance and Global Standards
Principle 5: Accountability
Principle 6: Accessibility and Inclusion
Principle 7: Sustainability

Principle 6: Accessibility and Inclusion

Technology adoption should support government's broader societal goals.

Accessibility

How can cloud help my organization meet its mission and performance indicators?

One major benefit of cloud computing is that smaller public sector agencies can access the same computing resources as the largest governments. Emerging-country governments can access world-class infrastructure without having to build it themselves. All government agencies, regardless of size, can access the IT resources they need when they need them without having to invest in all the physical plant that was historically required. In the private sector, this phenomenon has been referred to as the "democratization of IT,"[67] but the term is equally applicable to government.

The benefits are more than just financial. Governments are responsible to deliver services to citizens in a way that optimizes public resources. But they also have objectives that go beyond mere cost-savings. Civil service agencies are measured on many indicators, including human development goals, citizen protection and safety, peaceful foreign relations, and social and cultural preservation and development.

Technologies that cloud computing enable can contribute to achieving these goals in many ways. Data analytics solutions improve road transport networks, circulation patterns and public transit systems using sensors and citizen-submitted data. Internet of Things ("IoT") products enable health care providers to shift health services from reactive approaches of the past to preventative and continuous patient care paradigms, increasing wellness and healthy life expectancy. Perhaps the most immediate benefits of cloud in the public sector are in increased citizen access to services.

Artificial intelligence ("AI"), which is powered by cloud computing, is well-poised to increase access to government services. Many citizen services consist of answering questions, processing forms, drafting documents and other routine tasks, which are precisely the activities that AI is best at.[68] For example, virtual assistants (AI-powered chatbots) like Jamie in Singapore is a public-facing tool that helps users to receive instant service response, without worrying about high-volume bottlenecks associated with call centers.[69] Roxy in Australia is a similar internal tool that enables civil servants to find information and respond faster to citizen queries.[70]

[67] "Why Your Cloud Strategy Matters", Forbes, 30 September 2016, at https://www.forbes.com/sites/gartnergroup/2016/09/30/why-your-cloud-strategy-matters/#7d10bb6965b6

[68] Hila Mehr, "Artificial Intelligence for Citizen Services and Government", Ash Center for Democratic Governance and Innovation, August 2017, at https://ash.harvard.edu/files/ash/files/artificial_intelligence_for_citizen_services.pdf.

[69] "Jamie Virtually Knows Everything", Open Gov Asia, 6 August 2018, at https://www.opengovasia.com/jamie-virtually-knows-everything/.

[70] "Introducing Centrelink's robo-public servant", The Sydney Morning Herald, 17 January 2017, at https://www.smh.com.au/public-service/introducing-centrelinks-robopublic-servant-20170117-gtt2na.html.

Inclusion

Cloud computing also powers technology that drives inclusion of citizens that are often marginalized.

For example, one in seven of the world's population has some form of disability.[71] Technology has long been instrumental in helping these people engage more fully. Still, studies have repeatedly found that labour force participation for persons with disabilities is significantly lower than for people without disabilities.[72] And, all other things being equal, for people with disabilities who are able to find employment their wages tend to be lower.[73] Their decreased economic power translates into less political influence and decreased access to educational, health and government services.[74]

New cloud-based technologies could help to solve this. AI can be a powerful tool for increasing access to information, education, employment, government services, and social and economic opportunities. Real-time speech-to-text transcription, visual recognition services, and predictive text functionality, which suggests words as people type, are examples of AI-enabled services that are already empowering those with hearing, visual and other impairments.

Other groups and services are also benefited when governments adopt cloud. Educational software adapts exercises to students' ability and signals to teachers which students need extra help before those teachers can spot the problem themselves. Poorer and rural citizens can access government services on a round-the-clock basis, which is more conducive to shift-workers and people living in remote communities.

Thoughtfully deployed, the accessibility and inclusionary advantages of cloud-based technology can produce a disproportionately positive impact on people in emerging economies, remote locations and impoverished communities. Recognizing this, United Nations agencies have embraced AI and other cloud-based technologies as accelerators for realizing the 2030 Agenda for Sustainable Development and as a significant contributor to several of the Sustainable Development Goals.[75]

Recommendations

Policymakers should	Procuring Agencies should
1. Advocate assessment mechanisms for potential IT solutions based not just on price, but on overall value to the agency, including accessibility and inclusion assessment criteria.	1. Discuss long-term missions, objectives, and key performance indicators with cloud service providers and explore how cloud solutions can help achieve those transformational objectives.

[71] "New world report shows more than 1 billion people with disabilities face substantial barriers in their daily lives." World Health Organization, June 9, 2011, http://www.who.int/mediacentre/news/releases/2011/disabilities_20110609/en.

[72] WHO, 'World report on disability', 2011, at 237, at http://www.who.int/disabilities/world_report/2011/en/ ("World Report 2011"); ILO, 'World Social Protection Report: Building economic recovery, inclusive development and social justice 2014/2015', at 53, at https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_245201.pdf; ILO, 'Disability Inclusion Strategy and Action Plan 2014-2017', at 1, at https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---ifp_skills/documents/genericdocument/wcms_370772.pdf.

[73] World Report 2011, at 239, at http://www.who.int/disabilities/world_report/2011/en/.

[74] UN, "Economic empowerment through inclusive social protection and poverty reduction strategies", Conference of States Parties to the Convention on the Rights of Persons with Disabilities, Sixth Session, 17-19 July 2013.

[75] UNDP, 'Governments of the Future: Leveraging Innovation and New Technologies for the 2030 Agenda', February 12, 2018, at http://www.undp.org/content/undp/en/home/news-centre/speeches/2018/governments-of-the-future.html.

Principle 7: Sustainability

Technology should help improve environmental sustainability.

The amount of electronic data in the world is forecast to grow from 4.4 zettabytes in 2013 to 180 zettabytes[76] in 2025.[77] That will be equivalent to over 23,000 GB of data for every person on earth, or a number of gigabytes that is over 100 times the estimated number of grains of sand on all the beaches in the world. This data must be stored on servers and transferred via Internet cables and networking equipment, all of which consume energy. This will soon translate into data centers ranking among the world's largest users of electrical power.[78] Governments will need to consider how their data storage and use strategy impacts their sustainability profile.

How can cloud help me reach my sustainability obligations?

The impact of human activities on the environment, in large part driven by energy intensity and consumption, is a major problem that governments are struggling to deal with. Through the Paris Climate Accord, most countries have committed to "reach global peaking of greenhouse gas emissions as soon as possible…and to undertake rapid reductions thereafter."[79] The Paris Climate Accord recognizes the need to balance concerns associated with this goal on the one hand and sustainable-development and poverty-eradication objectives on the other hand.[80]

The US government's National Climate Assessment 2018 states that "while [climate-change] mitigation and adaptation efforts have expanded substantially in the last four years, they do not yet approach the scale considered necessary to avoid substantial damages to the economy, environment, and human health over the coming decades."[81] A special report from the Intergovernmental Panel on Climate Change estimated that carbon dioxide emissions from industry would need to be about 50–80% lower in 2050 compared to 2010 levels to limit global warming to 2°C and 65–90% lower in 2050 compared to 2010 levels to limit global warming to 1.5°C.[82]

Cloud computing providers can help governments manage the energy consumption demands associated with the explosive growth of data. Traditional data centers always need to have capacity to meet peak computing demand, even if peak demand is only reached a few times a year. Cloud services enable organizations to consume only what they need at a given moment, thereby reducing their overall energy consumption and minimizing excess capacity.

[76] 180 followed by 21 zeros.

[77] Economist, 'Data is giving rise to a new economy', May 6, 2017, at https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy.

[78] 'Greener datacenters for a brighter future: Microsoft's commitment to renewable energy', May 19, 2016, at https://blogs.microsoft.com/on-the-issues/2016/05/19/greener-datacenters-brighter-future-microsofts-commitment-renewable-energy/.

[79] Paris Agreement under the United Nations Framework Convention on Climate Change ("Paris Agreement"), Art. 4(1), at https://unfccc.int/files/meetings/paris_nov_2015/application/pdf/paris_agreement_english_.pdf.

[80] Paris Agreement, Preamble.

[81] USGCRP, 'Impacts, Risks, and Adaptation in the United States: Fourth National Climate Assessment, Volume II', 2018, at https://nca2018.globalchange.gov/

[82] IPCC, "Global Warming of 1.5°C, an IPCC Special Report on the impacts of global warming of 1.5°C above pre-industrial levels and related global greenhouse gas emission pathways, in the context of strengthening the global response to the threat of climate change, sustainable development, and efforts to eradicate poverty", October 2018, at C.2.3.

Cloud data centers are also more efficient than traditional data centers per unit of data. Studies have found that organizations can increase energy efficiency by up to 93% by moving to the cloud.[83] Many cloud service providers have been recognized for innovation in energy-efficient data center design.[84] Also, because they operate globally, cloud service providers can base decisions on data center locations on how conducive the surrounding climate and infrastructure are to energy efficiency.[85]

In addition to energy-efficient design and site selection, Bloomberg reports that the tech industry has become the biggest corporate buyer of renewable energy.[86] The major cloud service providers have all committed to power their operations with 100% renewables.[87] Consequently, the carbon footprint of cloud services is even lower than energy-efficiency statistics alone would indicate. The studies cited above found that the cloud was up to 98% more carbon-efficient than on-premises software.[88]

Finally, cloud-based technologies do not just contribute to lower energy intensity in IT services; they can also play valuable roles in reducing energy consumption elsewhere. Data analytics and machine learning solutions for buildings and urban environments can reduce energy consumption with more fine-tuned cooling, heating and lighting systems. They can reduce fossil fuel emissions by improving traffic flows and optimizing smart-grid power distribution networks. IoT technologies can improve systems performance by continuously monitoring operations, controlling waste, and identifying maintenance needs with precision. Cloud solutions are even helping improve agricultural yields, enabling economies to meet growing food demands by providing insights into how crop and livestock yields can be increased while better controlling resource intensity, including land and water use.

Recommendations

Policymakers should	Procuring Agencies should
1. Encourage cloud service providers' commitments and measurable deliverables on sustainability to be incorporated into assessment criteria for procurement exercises.	1. Explore with providers how cloud services can help achieve your agency's objectives and obligations for sustainable development, energy-efficiency and reducing carbon emissions.

[83] The Carbon Benefits of Cloud Computing: A Study on the Microsoft Cloud. Microsoft, at https://blogs.microsoft.com/on-the-issues/2018/05/17/microsoft-cloud-delivers-when-it-comes-to-energy-efficiency-and-carbon-emission-reductions-study-finds/ (Carbon Benefits of Cloud Computing"). See also It's Greener in the Cloud. Amazon Web Services, at https://aws.amazon.com/about-aws/sustainability/ ("It's Greener in the Cloud").

[84] 'Green Awards, Recognition, and Advocacy', Equinix, at https://www.equinix.com/company/green/green-awards/; 'Microsoft sank a data center in the ocean. On purpose.', Treehugger, 3 February 2016, at https://www.treehugger.com/clean-technology/microsoft-sank-data-center-ocean-purpose.html; "DeepMind AI reduces energy used for cooling Google data centers by 40%", at https://www.blog.google/outreach-initiatives/environment/deepmind-ai-reduces-energy-used-for/.

[85] ' The reasons why Ireland is Europe's data center hub', Interxion, 15 November 2016, at https://www.interxion.com/blogs/2016/11/the-reasons-why-ireland-is-europes-data-centre-hub/.

[86] ' From Google to Facebook, Big Data Is Driving Green Energy Shift', Bloomberg, 13 November 2018, at https://www.bloomberg.com/news/articles/2018-11-13/google-facebook-drive-green-power-developments-with-ppa-deals.

[87] ' Apple, Google, Microsoft, and Amazon Support Clean Power Plan in Court Filing', Greenpeace, 1 April 2016, at https://www.greenpeace.org/usa/news/apple-google-microsoft-amazon-support-clean-power-plan-court-filing/.

[88] See Carbon Benefits of Cloud Computing and It's Greener in the Cloud, note 83 above.

Summary: Principles and Recommendations

This paper has introduced a set of seven principles with accompanying recommendations for policymakers and procurement agencies. While the recommendations for policymakers intend to help policymakers develop procurement rules and policies, the recommendations for procurement agencies consider how to implement these in practice. These principles and recommendations should be followed to facilitate cloud adoption in the public sector:

Recommendations

<table>
<tr><th colspan="2">Principle 1: Security
Information management systems security is fundamental for the public sector.</th></tr>
<tr><th>Policymakers should…</th><th>Procuring Agencies should…</th></tr>
<tr><td>General
1. Expressly recognize the generally greater security offered by cloud-based systems over on-premises systems.
2. Require cloud services' security profile and performance to be assessed using the security profile of the current IT environment as a benchmark.
Data Classification
3. Advocate appropriate data classification according to existing state secrecy laws.
Data Localization
4. Not require data localization on security grounds.
Data Segregation
5. Recognize physical segregation and logical segregation as equally secure. Only for extremely sensitive data where security concerns overwhelm all other considerations should physical data segregation be required in addition to, not in place of, logical segregation.</td><td>General
1. Engage with cloud service providers early in the procurement process to understand how cloud solutions can help keep your systems and data safe and secure.
2. Ensure that tender requirements focus on overall security outcomes rather than prescribing specific security measures that might be incompatible with cloud solutions.
3. Where a cloud solution is at least as secure as your existing environment, do not preclude the solution on security grounds.
4. If your existing environment has been demonstrated to be insufficiently secure, prepare objective, technology-neutral and relevant security criteria before measuring all potential solutions – on-premises and cloud – against them.
Data Classification
5. Take a risk-based approach to data classification, having considered the risks of impact to national security associated with unauthorised disclosure and access. Classification should not be based on the source or the nature of the information or other criteria.
6. Bear in mind the risks of underclassifying and overclassifying data.</td></tr>
</table>

Recommendations

<table>
<tr><th colspan="2">Principle 1: Security
Information management systems security is fundamental for the public sector.</th></tr>
<tr><th>Policymakers should…</th><th>Procuring Agencies should…</th></tr>
<tr><td></td><td>Data Localization
7. Not introduce data localization requirements on security grounds without first conducting an objective analysis and determining that the extreme sensitivity of the data in question and any security benefits of having data located in a segregated facility clearly outweigh the drawbacks and risks, including security risks, that are associated with data localization.
8. Discuss with cloud service providers what technical, legal, and other measures they have in place, including as it relates to law enforcement and government access, to ensure data remains adequately secured and within your control given that data's sensitivity.</td></tr>
<tr><th colspan="2">Principle 2: Privacy and Personal Information
Governments need to ensure that privacy rights are respected.</th></tr>
<tr><th>Policymakers should…</th><th>Procuring Agencies should…</th></tr>
<tr><td>1. Require appropriate due diligence into privacy practices and policies of cloud service providers to ensure that personal data is no less protected with the cloud service provider than it is with the collecting agency.
Privacy and Security
2. Carefully distinguish between security and privacy considerations.
3. Not introduce data localization requirements on privacy grounds.</td><td>1. Have open discussions with cloud service providers about privacy practices and how moving to the cloud can help enhance personal data protection and control over government information systems.</td></tr>
</table>

Recommendations

<table>
<tr><th colspan="2">Principle 3: Availability, Integrity and Resilience
Governments need information and technology to be reliable.</th></tr>
<tr><th>Policymakers should…</th><th>Procuring Agencies should…</th></tr>
<tr><td>1. Require adequate due diligence of cloud service providers' availability statistics and infrastructure, integrity and verification tools, and service level agreements.
2. Require performance benchmarks to be set against existing systems.</td><td>1. Have open discussions with cloud service providers about infrastructure, integrity and verification tools, service availability and other available means of ensuring that cloud solutions provide the same or greater availability, integrity and resilience compared to self-managed, on-premises systems.</td></tr>
<tr><th colspan="2">Principle 4: Regulatory Compliance and Global Standards
Technology solutions must be measured to clear, verifiable benchmarks for quality and service reliability.</th></tr>
<tr><th>Policymakers should…</th><th>Procuring Agencies should…</th></tr>
<tr><td>1. Encourage adoption of applicable international standards rather than creation of unique requirements at the national or agency level.
2. Permit and encourage contracting using the cloud service provider's standard contracts.</td><td>1. Require cloud service providers to provide evidence that they hold appropriate certifications and do not request audit rights to check measures that are covered by those certifications.</td></tr>
<tr><th colspan="2">Principle 5: Accountability
Technology procurement must align to agencies' duty of accountability.</th></tr>
<tr><th>Policymakers should…</th><th>Procuring Agencies should…</th></tr>
<tr><td>1. Recognize and allow that any major IT restructuring project will be dynamic and that there will be learnings along the way and as technology and needs change.</td><td>1. Conduct comprehensive IT planning internally and consult early and on an ongoing basis with compliance departments, supreme audit institutions and cloud service providers to develop your overall cloud computing strategy.
2. Update performance indicators as necessary in consultation with the stakeholders mentioned above.</td></tr>
</table>

Recommendations

<table>
<tr><th colspan="2">Principle 6: Accessibility and Inclusion
Technology adoption should support government’s broader societal goals.</th></tr>
<tr><th>Policymakers should…</th><th>Procuring Agencies should…</th></tr>
<tr><td>1. Advocate assessment mechanisms for potential IT solutions based not just on price, but on overall value to the agency, including accessibility and inclusion assessment criteria.</td><td>1. Discuss long-term missions, objectives, and key performance indicators with cloud service providers and explore how cloud solutions can help achieve those transformational objectives.</td></tr>
<tr><th colspan="2">Principle 7: Sustainability
Technology should help improve environmental sustainability.</th></tr>
<tr><th>Policymakers should…</th><th>Procuring Agencies should…</th></tr>
<tr><td>1. Encourage cloud service providers’ commitments and measurable deliverables on sustainability to be incorporated into assessment criteria for procurement exercises.</td><td>1. Explore with providers how cloud services can help achieve your agency’s objectives and obligations for sustainable development, energy-efficiency and reducing carbon emissions.</td></tr>
</table>

The ACCA is a leading industry association comprising the stakeholders of the cloud computing ecosystem in Asia. The ACCA works to ensure that the interests of the cloud computing community are effectively represented in the public policy debate.

Our primary mission is to accelerate the growth of the cloud market in Asia, where we promote the growth and development of cloud computing in Asia Pacific through dialogue, training, and public education.

Through regular meetings, we also provide a platform for members to discuss implementation and growth strategies, share ideas, and establish policies and best practices relating to the cloud computing ecosystem.

ACCA Member Companies

ADN Telecom

aws

cisco

DIGITAL REALTY

EQUINIX

HSBC

Google

Microsoft

salesforce

TrustSphere Because Relationships Matter

Join us as a member today!

✉ secretariat@asiacloudcomputing.org

🌐 asiacloudcomputing.org

@accacloud

ISBN 978-981-14-1656-9

9 789811 416569