National Cloud Computing Legislation Principles:

Guidance for Public Sector Authorities Moving to the Cloud

Stephen Mutkoski
Legal and Corporate Affairs Department
Microsoft Corporation
Redmond, USA
Steve.mutkoski@microsoft.com

Abstract— **Governments around the world are actively seeking to leverage the many benefits of cloud computing while also ensuring that they manage risks that deployment of the new technologies can raise. While laws and regulations related to the privacy and security of government data may already exist, many were drafted in the "pre-cloud" era and could therefore benefit from an update and revision. This paper explores some of the concepts that should be incorporated into new or amended laws that seek to guide public sector entities as they move their data and workloads to the cloud.**

Index Terms—**Cloud Computing, Security, Public Sector, Risk Management, Regulation and Legislation.**

I. Introduction

As governments have increasingly begun to explore and use cloud computing technologies for public sector computing needs, they have also begun to look at the task of updating existing legal and regulatory frameworks that govern the protection of public sector data and computer systems.[1] This activity raises the important questions, what should "national cloud legislation" look like and are there any best practices that governments should seek to follow? It is important to note at the outset that public sector authorities in most jurisdictions could purchase and deploy cloud services today, without the need for any new legislation or regulation. But in many instances, while existing legislation or regulation permits use of cloud computing, it does little to encourage responsible risk management and thus actual adoption of new technologies such as cloud computing.[2]

Recognizing that legislation can often fail to keep pace with new technology, this paper recommends that legislation should establish and articulate basic principles regarding government use of cloud computing that can in turn guide agencies or ministries in their creation of more detailed regulations (which can be more readily updated to maintain alignment between the principles and new developments in technology). Key principles for national cloud legislation to help guide public sector authorities for creating workable cloud regulations are:

(1) Articulation of "Cloud First" vision and objectives for adoption of cloud computing
(2) Ensuring choice in cloud architecture
(3) Information system security requirements and assurance
(4) Data privacy requirements and assurance
(5) Data governance and classification practices and
(6) Transitional issues caused by a "Cloud First" Strategy

II. Legislating "Cloud First" Principles in Procurement

Cloud computing holds exceptional promise for governments and for national advancement led by government's innovative use of cloud computing.[3] But public sector use of cloud computing technologies raises some serious issues around control and handling of sensitive government data and there is an emerging consensus among central governments that public sector migration to cloud computing should be carefully regulated. The initial step in that regulatory process is often national legislation (or an executive branch decree), that both helps create the impetus for the move to cloud computing and sets out the areas of risk that must be addressed by public sector authorities as they move the cloud.[4]

Cloud computing legislation should provide a framework that results in public sector authorities embracing cloud computing where appropriate, leading to an approach that many have referred to as "Cloud First."[5] By using cloud services, governments can achieve far greater computing power, greater availability and resilience of data, and improved security even as they dramatically reduce their IT costs.[6] Most importantly, scalable, on-demand cloud computing services can help government organizations focus on key public priorities with increased agility.[7] In addition to direct cost savings for the government, government use of cloud computing can encourage national use of a technology that is proven to empower new job creation, democratize computing and social inclusion, and increase national competitiveness.[8]

Reliance on existing legacy systems, concerns about security and privacy and general risk aversion are frequently cited as barriers to cloud adoption by government agencies and ministries.[9] Legislation can help break this logjam by more clearly empowering public sector authorities to chart their individual path to the cloud via an internal risk assessment and management process. Cloud legislation should require that regulations enacted by public sector authorities specifically address risk management processes and clarify that each agency or ministry will determine where cloud computing is appropriate, through understanding and managing risks associated with cloud computing use with regard to specific data that the agency or ministry maintains.

978-1-4799-8218-9/15 $31.00 © 2015 IEEE
DOI 10.1109/IC2E.2015.104

But legislation should go further and require public sector authorities to set meaningful goals for cloud use. Legislation should direct public sector authorities to create regulations that require a presumption of cloud use or impose meaningful deliverables and milestones, for instance migration of specific types of data or workloads to the cloud or multi-year targets for percentage of budget spent on cloud computing technologies. Requiring agency and ministry regulations to incorporate such concrete benchmarks will ensure that deployment and use of cloud technologies becomes a reality.

Suggested Legislative Language: "Cloud computing holds exceptional promise for governments and for national advancement led by government's innovative use of cloud computing. All government agencies are directed to create a "Cloud First" policy that establishes cloud computing as the preferred ICT deployment strategy. Such policies shall include a risk-based process for determining where cloud computing may be appropriate and what security requirements will be necessary for its use. The agency policy or regulations governing the use of cloud computing should also set appropriate targets for use of cloud computing within the agency to ensure that progress is made over time."

III. Ensuring Cloud Service Model Choice for Public Sector Authorities

Cloud computing is a term that encompasses many diverse computing models, from public cloud to private cloud to hybrid clouds, with new models or variants springing up as technology continues to evolve.[10] Each of these models present different costs and benefits as well as different risk profiles.[11] But the long history of public sector IT procurement suggests that no single model will necessarily meet all needs, especially for the diverse range of public sector authorities that make up a typical national government.

With different levels of sensitivity of data and workloads across different government agencies or ministries, it is unlikely that the public cloud model alone will meet all government needs. But it is likely equally true that not all public sector authorities will benefit from restricting themselves to private cloud or on premises solutions. The various security, cost and national sovereignty issues presented by these different models creates a complicated matrix, one that ultimately can benefit from the deep expertise of agencies and ministries who have a long history of safeguarding their own data and workloads.[12]

Requiring public sector authorities to use only a single cloud model will likely result in loss of some or all of the benefits that the government is seeking by moving to the cloud. As a result, national cloud legislation should promote choice and enable agencies and ministries to select cloud architectures that are fit for purpose, taking into account data and workload sensitivities and cost/benefit and risk profiles of various cloud models. In many agencies and ministries, this will result in a mix of public, private and even traditional on-premises computing models.

Suggested Legislative Language: "Agency regulations should address risks related to various service models of cloud computing, including public cloud, hybrid cloud and private cloud service models. Given the wide range of government data and workloads, those regulations should include provisions which allow the agency to match sensitivity of various government data and workloads with the appropriate cloud computing service model."

IV. Legislative Guidance on Information System Security Requirements

Risk assessment related to security issues is critical when considering a move to the use of cloud computing technologies, but it should not paralyze an agency or ministry and prevent them from making meaningful deployment and use of cloud computing technologies.[13] Enabling legislation should direct public sector authorities to incorporate practical security requirements into regulations, focusing both on substantive security requirements (and defined security controls that address those requirements) as well as the process associated with verifying that such requirements and controls are met by a particular system or service provider. Legislation should also highlight that public sector objectives for moving to the cloud can be best met if these security requirements are drafted with reference to a growing body of international standards and certifications.

A. Security Requirements and Controls

A key element of successful public sector adoption and use of the cloud is ensuring that essential security requirements are identified and security controls to address those requirements are implemented by cloud systems that the government will use. Public sector regulations must therefore include reference to an array of substantive security functional requirements, including in such areas as "identity & access control," "management & monitoring" and "information protection."[14] Cloud regulations should focus in the first instance on the globally consistent requirements that are shared by public sector (and even many private sector) users of cloud computing technologies around the world. Because cloud computing is based on aggregation and scale to drive down cost, using these shared requirements as a baseline will ensure that public sector authorities craft requirements that are consistent with a sizeable component of the existing marketplace of cloud providers. Rather than each agency or ministry "reinventing the wheel," public sector regulations should draw from the growing commons of government cloud requirements and related controls.[15]

The regulation drafting process conducted by agencies and ministries should also include consideration of whether the public sector authority (or the government in their country as a whole) has any "unique" substantive security requirements. Those include requirements that take into account environmental factors (e.g., an island nation such as the Philippines may have a unique requirement when it comes to data center continuity requirements, such as the minimum separation of two data centers) and geopolitical factors (e.g., a country in an area with active conflict or political turmoil may have requirements about how data may be routed between regional data centers). These unique substantive requirements may exist, but public sector authorities should consider a cautionary principle: Creation of too many unique requirements will ultimately come into tension with one of the essences of cloud computing-- consistent requirements in high volume drive cost down dramatically—a tension that may increase cost to government for cloud services or preclude their use entirely.

B. Security Verification Process Requirements: Service Provider "Assurance"

In addition to specifying security requirements, public sector regulations should outline the process for affirming or verifying that such requirements are met by service providers. Several governments have outlined such processes and there are some best practices emerging that other governments can follow.[16] One important lesson that is emerging is that the verification process should draw from the pool of existing international certifications and accreditations, as opposed to starting entirely anew. This concept of "reuse" of existing certifications enables public sector authorities to build off existing global certification assets, including detailed audit reports, and avoid creating cumbersome internal processes that will slow cloud adoption and likely add very little beyond what existing certifications and audit reports would show.

But more broadly, public sector regulations should establish a verification process based on the principle of "assurance." Assurance encompasses a number of common sense approaches to verification, and depending on the nature of the specific requirement, the assurance process could be any one of the following approaches (or a combination of them):

•Service provider assertion: At the most basic level, the service provider should offer descriptions of how their service operates and whether and how the provider believes it meets substantive security requirements. There are many "binary" requirements (yes service does x, no service doesn't do y) that public sector authorities may be willing to accept at face value, taking into account the service provider's reputation and level of maturity around security and past interaction with that service provider.

•Contractual commitment: An additional layer of confidence may be gained for certain requirements by requiring that the service provider contractually commit to meeting the requirement(s). Public sector authorities may want to include in their regulations the specific commitments to security requirements which it will want cloud providers to meet, so that those commitments are standardized across all cloud procurements.

•Independent validation of assertions through certification: For certain requirements, it may be the case that the public sector authority would like assurance from a third party as to whether and how a service provider meets a security requirement. The most common avenue for such independent validation is via reference to a certificate of compliance with a recognized standard—including information about the scope of the certification audit and applicable audit reports that provide more detail about applicable security controls. Given the growth of international security standards, the assurance process established by a public sector authority can lean heavily on existing independent certifications (and the supporting documents such as audit reports).[17] Assurance related to the vast majority of security requirements can successfully and reliably accomplished via a combination of the first three mechanisms (assertion, contractual commitment and/or independent certification.

•Independent testing: There may be a small number of unique security requirements for which an existing independent certification does not exist. In such cases, public sector authorities should consider whether service provider assertion and contractual commitments are sufficient or whether they should impose an independent testing requirement to verify the unique security requirement.

Suggested Legislative Language: "Agency regulations for cloud computing should address security functional requirements in the first instance by referencing globally consistent requirements that are shared by public sector users of cloud computing technologies around the world. Regulations should also establish a process based on the principle of 'assurance' that verifies such security requirements are met, including through reference to service provider assertions, contractual commitments and independent validation through certifications."

V. Legislative Guidance on Data Privacy Requirements

Security requirements are often the first line of concern as customers begin the journey to the cloud, and it certainly makes sense that securing systems and data from unauthorized third parties is of such great concern. But national cloud regulations must look beyond access by unauthorized parties and should also address issues of permitted uses by authorized third parties. Whether framed as data protection or data privacy requirements, regulations should include clear restrictions on use of government data by service providers. Enabling legislation should mandate that cloud regulations incorporate restrictions that prohibit cloud service providers from using government data for purposes other than providing the specific contracted service or services and restrictions on using any government data for advertising related purposes.[18]

New data protection standards for cloud computing, such as ISO 27018 are now emerging to help customers articulate data privacy requirements, as well as to give third party verification and auditability of such requirements.[19]

Suggested Legislative Language: "Agency cloud regulations should include restrictions on service provider use of government data, prohibiting cloud service providers from using government data for purposes other than providing the specific contracted service and an express restriction on using any government data for advertising related purposes."

VI. Data Governance and Data Classification

Data privacy and security requirements are constructs that while crafted inside the public sector authority are almost exclusively directed outside the government, at the cloud service provider. But there are important requirements that public sector authorities must impose on themselves as they begin their move to the cloud. One of those requirements relates to creating an inventory of and classification for the various workloads and data sources that a public sector authority manages. Public sector data and workloads are not homogenous, and will raise distinct privacy and security issues. Creating and inventory and classification of data and workloads is an essential step for public sector authorities as they move to the cloud.[20]

As one lawmaker noted "Storing benign information on internal [Department of Defense] services is an increasingly large expense, particularly given the widespread availability of secure, fast, reliable and affordable storage services utilized in the private sector."[2] This comment highlights the need for robust data classification within agencies and ministries, to ensure that such benign information is not treated in the same manner as information which raises national security or sovereignty issues.

Enabling legislation should ensure that public sector cloud regulations include a requirement that the public sector authority implement a data governance and data classification framework as part of its move to the cloud. Data governance and data classification allows public sector authorities to identify differing sensitivity levels in data and workloads and create rules for how each level of information should be treated. In the context of cloud computing, this allows public sector authorities to specify relevant security controls and processes for sensitive data that will be moved to the cloud but also potentially identify a certain class of highly sensitive government data that raises national sovereignty concerns and is suitable only for on-premises or private cloud systems.

Suggested Legislative Language: "Agency cloud regulations should establish an appropriate data governance framework which includes a classification system for agency data and workloads and allows the agency to determine which data and workloads will be suitable for various service delivery models, including public cloud, hybrid cloud, private cloud and even on premises models."

VII. Transitional issues caused by a "Cloud First" Strategy

Although a presumption of cloud use and defined targets and goals for that use are important, the process of transitioning to the cloud may disrupt or create tension with well-established procurement, budgeting and organizational practice. Legislation should acknowledge this disruption and direct agencies to develop procurement rules that allow cloud service to be acquired efficiently and ensure that their budget practices can support the variable cost (or cost savings) of on-demand cloud services.

Finally, effective use of the cloud will require new skills from all of the people that support government use of information technology. Support for providing those new skills and awarding those who acquire them has proven to advance the use of cloud computing.[21] Accordingly, public sector authorities should ensure cloud regulations and policies address these skills, staffing and personnel issues.

Suggested Legislative Language: "Agency regulations should address budgeting, personnel and retraining issues that will likely arise as the agency adopts cloud computing."

VIII. Conclusions

Recognizing that legislation can often fail to keep pace with new technology, this paper recommends that legislation should establish and articulate basic principles regarding government use of cloud computing that can in turn guide agencies or ministries in their creation of more detailed regulations (which can be more readily updated to maintain alignment between the principles and new developments in technology). Key principles for national cloud legislation that will ensure public sector authorities have sufficient guidance for creating workable cloud regulations include: (1) Articulation of "Cloud First" vision and objectives for adoption of cloud computing, (2) Ensuring choice in cloud architecture, (3) Information system security requirements and assurance, (4) Data privacy requirements and assurance, (5) Data governance and classification practices and (6) Transitional issues caused by a "Cloud First" Strategy.

Acknowledgment

I would like to thank Microsoft colleagues Gregg Brown and Scott Edwards for their review of and contributions to earlier drafts of this paper.

References

[1] There are several of new instances of cloud legislation being introduced around the world, and many of those focus in the first instance on where government data may be located, who may operate such services or requirements for transmitting such data across borders. See, Russian Parliament Draft Bill No 467078-6 (requirements for data location of state and municipal data) *available at* http://www.globaltradealert.org/measure/russian-federation-data-localisation-requirement-concerning-state-and-municipal-internet-sit and Jeferson Ribeiro, "Bill would allow Brazil to decree local Internet data storage" (November 5, 2013), *available at* http://news.yahoo.com/bill-allow-brazil-decree-local-internet-data-storage-204248032.html (allowing the creation of regulations on data location, leading to passage of Interministerial Ordinance No. 141 on May 2, 2014 which required that government IT services must be operated by the government).

[2] Jeffrey Roman, "Bill Pushes Cloud Computing for DoD" GovInfoSecurity (April 28, 2014), *available at* http://www.govinfosecurity.com/bill-pushes-cloud-computing-for-dod-a-6795.

[3] Sujatha Perepa, "Why the US Government is Moving to Cloud Computing" Wired Magazine (September 25, 2013), *available at* http://www.wired.com/2013/09/why-the-u-s-government-is-moving-to-cloud-computing/; Horacio E. Gutierrez & Daniel Korn, *Facilitando the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America*, 45 U.

Miami Inter-American L. Rev. 33, 39-44 (2014), *available at* http://inter-american-law-review.law.miami.edu/wp-content/uploads/2014/03/Facilitando-the-Cloud.pdf; European Commission, *Unleashing the Potential of Cloud Computing in Europe*, 2-5, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF.

[4] U.S. General Services Administration, "Cloud IT Services," (Nov 4, 2014), *available at* http://www.gsa.gov/portal/content/190333; Vivek Kundra, *Federal Cloud Computing Strategy* (Feb. 8, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

[5] Rohan Pearce, "Government Policy Mandates 'Cloud First' for Agencies" ComputerWorld Australia (October 9, 2014), available at http://www.computerworld.com.au/article/556994/government-policy-mandates-cloud-first-agencies/; UK Cabinet Office, "Government Adopts 'Cloud First' Policy for Public Sector IT" (May 5, 2013), *available at* https://www.gov.uk/government/news/government-adopts-cloud-first-policy-for-public-sector-it; Kundra, *Federal Cloud Computing Strategy*, at 1-2; David C. Wyld, *Moving to the Cloud: An Introduction to Cloud Computing in Government*, 18-31 (2009), *available at* http://www.ukeig.org.uk/sites/default/files/WyldCloudReport_0.pdf..

[6] Patricia Moloney Figliola and Eric A. Fisher, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management*, Congress Research Service (CRS) Report 7-5700, 6-7 (Jan. 20, 2015), *available at* http://fas.org/sgp/crs/misc/R42887.pdf; Darrell West, *Saving Money Through Cloud Computing (Brookings Institution,* April 2010), *available at* http://www.brookings.edu/~/media/Files/rc/papers/20100407_cloud_computing_west/0407_cloud_computing_west.pdf; European Commission, *Unleashing the Potential of Cloud Computing in Europe*, at 4-5.

[7] Kundra, *Federal Cloud Computing Strategy*, at 8-9; Gutierrez & Korn, *Facilitando the Cloud*, at 43-44.

[8] Gutierrez & Korn, *Facilitando the Cloud*, at 39-43; John F. Gantz, *Cloud Computing's Role in Job Creation*, IDC White Paper, March 2012, *available at* http://people.uwec.edu/HiltonTS/ITConf2012/NetApp2012Paper.pdf; Joanna Gordon et al., *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driving Transformation*, World Economic Forum (2010), *available at* http://www3.weforum.org/docs/WEF_ITTC_FutureCloudComputing_Report_2010.pdf.

[9] Samuel Tweneboah-Kuduah, Dr. Barbara Endicott-Popovsky &Anthony Tsetse, *Barriers to Government Cloud Adoption*, 6 International Journal of Managing Information Technology 3, 9-10 (Aug. 2014), *available at* http://airccse.org/journal/ijmit/papers/6314ijmit01.pdf; KPMG, *Exploring the Cloud: A Global study of Governments' Adoption of Cloud*, 16 (2012), *available at* http://www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicaciones/Documents/Exploring-the-Cloud.pdf.

[10] Sasha Segall, *Jurisdictional Challenges in the United States Government's Move to Cloud Computing Technology*, 23 Fordham Intell. Prop. Media & Ent. L.J. 1105, 113-114 (2013); J. Nicholas Hoover, *Compliance in the Ether: Cloud Computing, Data Security and Business Regulation*, 8 J. Bus. & Tech. L. 255, 258 (2013); Mariana Carroll, Alta van der Merwe, and Paula Kotze, *Secure Cloud Computing: Benefits, Risks and Controls*, Information Security South Africa, 2 (2001), *available at* http://icsa.cs.up.ac.za/issa/2011/Proceedings/Full/13_Paper.pdf.

[11] KPMG, *Exploring the Cloud: A Global study of Governments' Adoption of Cloud*, at 9; Figliola & Fisher, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative*, at 2-5; Wayne Jansen & Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, NIST Special Publication 800-144, 3-13 (Dec. 2011), *available at* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494; Johnny Barnes, "Public vs. Private vs. Hybrid Computing and Storage Clouds" IBM Center for the Business of Government, (March 21, 2011), *available at* http://www.businessofgovernment.org/blog/strategies-font-color-redcut-costsfont-and-improve-performance/private-vs-public-vs-hybrid-comp).

[12] Richard Spires, *Cloud Computing, Front and Center*, CIOC Blog (Sept. 6, 2011), available at https://cio.gov/cloud-computing-front-and-center.

[13] Howard Baldwin, "Public Sector Cloud Computing: The Good, The Bad and The Ugly," ComputerWorld (May 9, 2012), available at http://www.computerworld.com/article/2503858/cloud-computing/public-sector-cloud-computing--the-good--the-bad-and-the-ugly.html; KPMG, *Exploring the Cloud: A Global study of Governments' Adoption of Cloud*, at 33.

[14] UK National Technical Authority for Information Assurance, "Implementing Cloud Security Principles" (Aug. 14, 2014), *available at* https://www.gov.uk/government/publications/implementing-the-cloud-security-principles/implementing-the-cloud-security-principles#operational-security; Wayne Jansen & Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, NIST Special Publication 800-144, 14-35 (Dec. 2011), *available at* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494.

[15] European Commission, *Unleashing the Potential of Cloud Computing in Europe*, at 10-11; Figliola & Fisher, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative* (describing U.S. standards organization including FedRAMP and SAJACC).

[16] Tweneboah-Kuduah, Endicott-Popovsky & Tsetse, *Barriers to Government Cloud Adoption*, at 13-14; European Network and Information Security Agency (ENISA), *Cloud Computing Information Assurance Framework*, (Nov. 2009), *available at* http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework; NIST, *NIST Cloud Computing Security Reference Architecture*, NIST Special Publication 500-299, *available at* http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf.

[17] National Institute of Standards & Tech (NIST), http:/www.nist.gov/information-technology-portal.cfm (last visited Feb. 7, 2015); Cloud Security Alliance, https://cloudsecurityalliance.org (last visited Feb. 7, 2015); International Organization for Standardization,

http://www.iso.org (last visited Feb. 7, 2015); James Ryan, *The Uncertain Future: Privacy and Security in Cloud Computing*, 54 SANTA CLARA L. REV. 497, 522-23 (2014).

[18] Karen S. Evans, "Lawsuit Raises Red Flags for Government Cloud Users" InformationWeek Government (March 25, 2014), *available at* http://www.informationweek.com/government/cloud-computing/lawsuit-raises-red-flags-for-government-cloud-users/d/d-id/1127897.

[19] Jonathan A. Beckham, "ISO 27018- Data Protection Standards for the Cloud" The National Law Review" November 23, 2014; Gutierrez & Korn, *Facilitando the Cloud*, at 46-47.

[20] Kudra, *Federal Cloud Computing Strategy*, at 29-30. Elena Malykhina, "Feds Hesitate Moving IT Services to the Cloud" InformationWeek Government, September 11, 2014.; Federal Information Processing Standards ("FIPS") Publication 199, Feb. 2004, *available at* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[21] Tweneboah-Kuduah, Endicott-Popovsky & Tsetse, *Barriers to Government Cloud Adoption*, at 12; David C. Wyld, *Moving to the Cloud: An Introduction to Cloud Computing in Government*, 45-47 (2009), *available at* http://www.ukeig.org.uk/sites/default/files/WyldCloudReport_0.pdf.