

29 July 2024

Honourable Minister Ranil Wickremesinghe
Minister of Technology,
Ministry of Technology,
Level 11, Unit No: 1101, One Galle Face Tower, No 1 A, Centre Road, Galle Face,
Colombo 02, Sri Lanka

Dear Minister Ranil Wickremasinghe,

Subject: Asia Internet Coalition (AIC)'s Industry Comments on the Policy for the Adoption of Cloud Services by Government Organizations in Sri Lanka

On behalf of the [Asia Internet Coalition](#) (AIC) and its members, I am writing to express our sincere gratitude to the Ministry of Technology for allowing the AIC to submit comments on the **Policy for the Adoption of Cloud Services by Government Organizations in Sri Lanka**. We appreciate the Ministry of Technology for its proactive approach in prioritizing the procurement and adoption of cloud-based ICT solutions, aiming to enhance the efficiency, productivity, and resilience of government services.

The Asia Internet Coalition (AIC) a leading industry association of Internet and technology companies that promotes the understanding and resolution of Internet policy issues in the Asia Pacific region. Our mission is to represent the Internet industry and participate in and promote stakeholder dialogue between the public and private sectors, sharing best practices and ideas on Internet technology and the digital economy. For Honorable Minister's information, the AIC has previously commented on several policy areas in Sri Lanka including the Online Safety Act.

On this note, we believe that the proposed policy will significantly contribute to the digital transformation efforts of the Sri Lankan government. **While we commend these efforts, we would also like to take the opportunity so submit detailed comments and suggestions in Appendix I for your consideration.** We hope our insights will be valuable in shaping a comprehensive and effective policy that will drive the successful adoption of cloud services across all government entities in Sri Lanka.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Furthermore, we would also be happy to offer our inputs and insights on industry best practices, directly through discussions and help shape the dialogue for the advancement of cloud computing in Sri Lanka.

Thank you

A handwritten signature in blue ink, appearing to read "Paine".

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

APPENDIX I

Inputs to Sri Lanka's Policy for the Adoption of Cloud Services by Government Organizations in Sri Lanka

I. A comparison of cloud migration approaches, Section 5

Currently, the draft Policy classifies cloud service providers as the following and contrasts each along the listed policy priorities, with a clear preference for Government Cloud:

1. Government Cloud (Government Cloud)
2. Commercial Cloud in Sri Lanka (Local CSP)
3. Off-shore Cloud (International CSP)

Additionally, the comparative analysis of different CSP options does not adequately demonstrate the performance of CSPs along the policy priorities. We believe the following should be added:

Principle	Government Cloud	Cloud Service Providers (CSPs)
Data Security	Provides complete security protection for the infrastructure. In addition, client will be responsible for applying security precautions for the applications hosted in GOVERNMENT CLOUD.	The benefit of migrating government workloads and data onto to public cloud is the ability to enhance overall data security. Hyperscalers will meet international security standards, will be certified appropriately, and will abide by all relevant laws and industry standards.
Data Residency	Data sovereignty aspects are fully guaranteed in alignment with Sri Lankan legal and regulatory landscape.	The benefits of cloud are best realized when there are no data residency restrictions placed on data. Data residency restrictions undermine the economies of scale as well as the security benefits to be gained from shared computing infrastructure. Nevertheless, where agencies have concerns with extraterritorial access to Secret data, then the appropriate security standards and controls should be employed or the agency should work with the government to consider deploying a private, on-premise cloud solution.
Cost Optimization	Currently, offered on Free of Charge (FoC) basis. Planning to implement Pay-as-you-go model in the	Hyperscalers provide a pay-as-you-go model for all services and limit costs for government.

Principle	Government Cloud	Cloud Service Providers (CSPs)
	next version.	
Sustainability	This project is owned by GoSL and currently operated by ICTA thus, sustainability is guaranteed.	Hyperscalers help governments meet and exceed efficiency and carbon reduction targets. The cloud allows for the avoidance of over-provisioning workloads, thereby reducing resource consumption because these workloads resize to the demand load.
Transparency and Accountability	This project is owned by GoSL and currently operated by ICTA thus, transparency and accountability are guaranteed.	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer (i.e., the government agency) of the utilized service.
Operational Efficiency	Application or data can be accessed from anywhere supported with LGN or public internet connectivity.	Cloud enables more effective collaboration as agencies more easily share resources across institutions, allowing for greater efficiency, entrepreneurship, and creativity in delivering public services.
Scalability	Flexibility exists to upscale/ downscale resources based on the client request.	Public cloud helps governments meet and exceed efficiency and carbon reduction targets. The cloud allows for the avoidance of over-provisioning workloads, thereby reducing resource consumption because these workloads resize to the demand load.
Disaster Recovery and Business Continuity	Strong contract with principle service providers including local support and delegated Technical Account Manager (TAM). In addition, certified GOVERNMENT CLOUD technical support team is involved in day-to-day operations through the Network Operations Centre (NoC).	With centralized data storage, management, and backups, data retrieval and business recovery during times of crisis (e.g. natural disasters or other disruptive events) become faster, easier and more cost effective.

Scalability is essential for government services and public cloud is best positioned for it and provides the following benefits:

1. Spur innovation – Cloud computing allows government customers to access industry-shaping technology quickly, at an affordable cost, no matter what the scale. A successful Cloud First policy results in leading-edge IT environments that spur invention and innovation.

2. Faster deployment of services – reducing the amounts of ICT infrastructure required to be built and owned by government agencies reduces overall deployment times, and shifts the focus from management of infrastructure to delivery of services. Public ICT facilities and services can be tested and deployed quicker, and maintained more cost effectively, than if government agencies own and run unique computing facilities themselves.

3. New security models – Governments can obtain greater security in the cloud than is available in traditional data centers. The cloud enables customers to formalize account design, automate security and governance controls, and streamline auditing.

4. Greater budget control – A utility- based ‘pay for what you use’ model means that government agencies can purchase as much or as little resource as they need, as they need it. Cloud scalability results in systems usage being dialed up or down throughout the year as it is required. Transparency of the utility-based pricing structure means that spending caps and alerts can be implemented to further assist in budget control.

5. Decreased spending on legacy infrastructure – Deploying government services in cloud infrastructure results in immediate reductions of large capital outlays for ICT infrastructure and maintenance costs. Best of class services are made available to government agencies through cloud provisioning.

Recommendation – This type of classification of CSPs based on their nationality can create significant issues. Such classification stifles innovation by limiting competition and reduces the optionality of government agencies. This approach can compromise security and resilience and reduces diversity in service providers, which is crucial for a robust and secure IT infrastructure. It can lead to inefficiencies and higher costs for government services, as it narrows the pool of potential CSPs and reduces competitive pricing and innovative solutions that international providers might offer. Thus, avoiding classification based on nationality encourages a more open, competitive, and secure environment for cloud services. Government departments should be able to choose from best available CSP which comply with the stated policy objectives and provide the best set of services, security and cost to customers.

The draft Policy should refrain from favoring government cloud over public cloud solutions and overseas CSPs. Public cloud offerings provide superior security, agility, scalability, and cost-effectiveness, ensuring government agencies can leverage these while ensuring sovereignty and control. Embracing both public and government cloud options promotes a competitive environment that enhances overall efficiency and meets diverse agency needs effectively.

Additionally, we suggest adding the following section under Section 5:

Cloud Deployment Models

Public Cloud: *Public cloud services are operated by third-party cloud service providers, who own, manage, and deliver computing resources (e.g., compute, storage) over the internet. These computing resources are delivered to multiple organisations.*

Virtual Private Cloud (VPC): *A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud. VPC customers can run code, store data, host websites, and do anything else they could live in an ordinary private cloud, but the private Cloud is hosted remotely by a public cloud provider. VPCs*

combine the scalability and convenience of public cloud computing with the data isolation of private cloud computing.

Private Cloud Services: Government provides private cloud services and/ or dedicated government cloud that brings all cloud services into Data Centres managed and operated by Gov DC.

Hybrid Cloud: A hybrid cloud is a cloud computing environment that uses a mix of on-premises, private Cloud, and public cloud services with orchestration between these platforms. This typically involves connecting an on-premises data center to a public cloud. Some workloads cannot easily migrate to the Cloud since they need to work with large local datasets, share data with on-premises applications with single-digit-millisecond latency, or meet data residency requirements.

II. Cloud Implementation Process, Section 6

In the Figure 2 flowchart which outlines the process of cloud implementation, departments are guided to a "local CSP" for confidential or unclassified data. This is not aligned with globally accepted and conventional data classification practices.

Data classification is an important enabler to allow organizations to classify data based on sensitivity and operational impact and help Government decide what data goes on the cloud. Governments categorize their data based on its level of sensitivity and then manage each segment in a manner congruent with its level of sensitivity. It's important to keep in mind that Government should avoid over-classification as it could lead to overall weakening of security by spreading an organization's defenses over a much broader set of systems and data than is necessary. Moreover, an over-classification and reliance on data localization (as in the case of Sri Lanka's draft Policy) defeats the purpose of a cloud first approach. Most government data falls into low impact or official categories that can be deployed on the Cloud.

Classifying data into discrete categories enables the [Country] Government to better protect government information and make better-informed decisions with regard to access, storing and transmission of Government data. Data classifications achieve stronger outcomes for government agencies by clarifying the safeguards required for protecting different types of data, thereby reducing uncertainty, standardizing access, and reducing costs. It also enables business and other public sector agencies to be able to better use and manage appropriately classified data. Data can be broadly divided into three tiers of Public Sector Data Classification:

- Unclassified data, which can be stored on accredited public cloud
- Official data, which can be stored on accredited public cloud with encryption requirements;
- Secret and above, which may require private (on premise) cloud deployment with specific encryption requirements.

Government agencies are recommended to select the appropriate cloud deployment model according to an agency's specific needs, and the type of data it handles according to the Public Sector Data Classification, as illustrated in the table below. Depending on the classification of the agency's data, there will be a requirement to apply certain controls.

Recommendation: There should be only 2 scenarios for data classification: Secret and Unclassified data. The latter can be stored on the public cloud. In the case of Secret data, the applications and data can continue to be hosted in the existing setups or facilities (Govt Cloud/Dedicated Environments). In such cases, user departments may seek hybrid cloud architectures to integrate their on-premises IT systems with public cloud operations to support a broad spectrum of use cases.

We recommend adding the following in after Section 6.2

Strategic Planning: To achieve clarity when it comes to strategic objectives, it is a good practice to articulate it in the Introduction of a Cloud Services Request for Proposal (RFP);

1. The business objectives and benefits the organization seek to achieve by using the Cloud.
2. The structure of the framework agreement – who buys, who operates, who budgets, etc.
3. A clear understanding of the shared responsibility model between the public sector and cloud vendors is at the core of successful cloud purchasing and usage.
4. The type of relationship created between Cloud Service Providers (CSPs), distributors of marketplace services, consulting partners, Government procurement/contracting agencies, and government end-users.

III. Service Level Agreements, Section 8

We recommend adding the following at the beginning to Section 8:

Procurement Requirements and Considerations

As against the traditional model of defining fixed configurations & capacities and discovering fixed unit prices, commercial evaluation for Cloud has to be reframed so that the Departments can take advantage of the breadth of cloud services during the contract.

Unlike a traditional fixed bill of quantity and fixed price contracts, the clauses for Cloud contracting must be designed with the following fundamental principles:

1. Lift-and-shift procurement scenario: *Where the department is procuring only Cloud and managed services (and not a turnkey procurement that includes a solution).*

- a) *The overall Value (TCO) used for arriving at the L1 / Best Value Provider becomes an estimated contract value (maximum value of the contract). After commercial evaluation, the estimated contract value is not a payment commitment to the Service Provider.*
- b) *Embrace dynamic and public pricing, including access to CSP's price reductions. Optimize and consume from the breadth of cloud services within the maximum contract value and incorporate the ability to apply multiple discounting models during the contract.*
- c) *Variable OpEx Payments:*
 - i) *Paying for the resources that are consumed in the payment period. The contract value is only an estimated maximum of cumulative payments. Actual payments may range from 0% (in case of no provisioning of resources) to 100% of the contract value.*
 - ii) *Invoicing needs to factor in variable OpEx payments each month.*
- d) *Departments can continue to consume services (even beyond the original contract duration) if the cumulative payments don't exceed the contract's maximum value for both lift-and-shift and new solution procurement scenarios.*

2. Procurement for New Solutions (develop a new application on Cloud): *In scenarios where the service provider/application developer is responsible for developing the application and hosting, the solutioning should be left to the bidders.*

- a) *The cloud requirements should not be prescriptive. Cloud services should not be limited to computing and storage so that the bidders can architect using modern application design principles (e.g., micro-services architecture), leveraging the breadth of cloud services to design and propose an optimal cost solution.*
- b) *The department should only provide the performance-based / outcome requirements.*

Moreover, the Policy doesn't mention skilling for cloud-readiness anywhere. We think it is essential to build an understanding of the positive cultural changes and new skill-sets that come with cloud computing. The government agencies must review and update operations and employee skills to accommodate the change

in practices that come with a cloud migration. This includes ensuring that a government organization (or a partner) has the experience necessary to move workloads and applications to the cloud, and training/certifying staff en-masse for the required cloud skills. Industry can come together to support the government with skilling programs.
