GOVERNMENT CLOUD POLICY

DRAFT V 1.7

INFORMATION AND COMMUNICATION TECHNOLOGY AGENCY
OF SRI LANKA

VERSION HISTORY

VERSION	DATE	COMMENT
1.0	21.03.2022	Initial Draft
1.1	24.03.2022	First Review – Director, Policy
1.2	29.03.2022	First Review – Director, Infrastructure Services
1.3	30.03.2022	First Review – Director/Architect
1.4	01.04.2022	Second Review – Director, Infrastructure Services
1.5	04.04.2022	Third Review – Director, Infrastructure Services
1.6	19.04.2022	Fourth Review – Director, Infrastructure Services
1.7	26.05.2022	Review by the Security Team

LIST OF ABBREVIATIONS

CSP	Cloud Service Provider
GoSL	Government of Sri Lanka
LGC	Lanka Government Cloud
IaaS	Infrastructure as a Service
ICTA	Information and Communication Technology Agency
MoU	Memorandum of Understanding
MTTR	Mean Time to Repair
NDX	National Data Exchange
NSDI	National Spatial Data Infrastructure
PaaS	Platform as a Service
PT	Penetration Testing
SaaS	Software as a Service
TAM	Technical Account Manager
VA	Vulnerability Assessment
VMs	Virtual Machines

TABLE OF CONTENTS

1 INTRODUCTION

1.1 BACKGROUND

Government of Sri Lanka has recognized the importance of Digital Transformation in building an advanced, prosperous and inclusive nation. This directly follows the adaptation of emerging technologies, in order to become more efficient and productive in the information and service delivery. Data storage and connectivity in the public sector become decisive factors in ensuring that government services and information are available in a more agile, faster, cheaper, economical and secure manner. In view of that, the Government of Sri Lanka recognizes moving towards Cloud Infrastructure and Solution Services as a key enabler in making a shift from its traditional data storage and computing framework towards a more robust, effective, economical and secure landscape.

1.1.1 ON-PREMISE TO CLOUD

Many government organizations are heavily dependent on on-premise infrastructure for their Information and Communication Technology requirements. The maintenance and management of on-premise solutions is associated with sizeable costs as it requires in-house server and storage hardware, firmware, system integration tools, and human capital in order to continue with an uninterrupted operational flow.

As the government is committed towards the achievement of a digital transformation, exploring the possibilities of eliminating inefficiencies and facilitating a better service delivery; the government intends to take a paradigm shift from on-premise IT services to cloud services, being on par with the global trends in information and communication technology.

Cloud computing is increasingly recognized as a core technological aspect in digital transformation and innovation. The fundamental difference between on-premise services and cloud services lies in the technology, cost, maturity, reliability, sustainability, performance, better security etc. It is the most cost effective method to utilize, maintain and upgrade information systems infrastructure. Despite of incurring a massive cost for the maintenance of an on-premise infrastructure which requires expensive software and hardware; cloud solutions can be deployed with greater efficiency and cost reduction. Similarly, in an on-premise environment, infrastructure resides physically within the organization premises whilst in cloud environment, a third party service provider hosts the same for the organization and it brings less hassle for maintenance and operation.

1.1.2 DATA CENTRE USAGE

Data storage and use, supported by data centres, assists the governments to achieve their sustainability goals. In terms of data storage in an on-premise environment, a physical data centre becomes an intrinsic component. An on-premise data center/server rooms facilitate cloud infrastructure for an organization which consumes hardware, space, power, backup systems, environmental controls etc. needed to keep the servers functional. In a cloud data center, the actual hardware is managed and maintained by the cloud service provider. Clients host their applications and manage their data within a cloud infrastructure that runs on the cloud servers. These Tier III cloud data centres enables organizations to access faster innovation processes and flexible resources, and benefit from economies of scale, whilst storing data at much lower costs. As explained in the UNCTAD Digital Economy Report 2021[1], it is predicted that by 2025, 80% of global enterprises will shut down their traditional data centres and move to co-location data centres. Cloud data centres in comparison to the traditional on-premise data centres bring the following benefits to the surface.

- Lesser cost
- Scalable resources
- Elasticity
- Lesser procurement hassle
- Pay for what you use
- Less manpower requirement
- Rapid implementation
- Independent platform
- Easy remote access
- Higher security

1.1.3 CROSS BORDER DATA FLOWS

Governments recognize that innovations powered by cloud computing offer potential benefits and these innovations often require the movement of data across international borders. Striking a balance between facilitating a smooth flow of data and providing capabilities to preserve privacy, protect individual and public safety, and promote national security is a challenge. Governments face legal restrictions that limit their ability to store, transfer, and process data across borders, which include legal mandates to store data locally. In terms of the Sri Lankan context, data protection legislature pronounces the legal application on cross border data flow and the policy promotes the adoption of cloud computing in alignment and recognition of the respective legal principles enshrined in such legislation.

[1] https://unctad.org/system/files/official-document/der2021_en.pdf

1.1.4 EXPECTED OUTCOMES

Following outcomes are primarily expected by the government through successful adoption of cloud services within government organizations.

a. Cost benefit/saving

Application deployment on cloud infrastructure reduces the cost of purchasing, setting up, and maintaining technology services within the public sector. It offers government organizations the opportunity to streamline technology operations and improve efficiency in providing services.

b. Increasing government agility to respond to the needs of citizens and businesses

Cloud solutions allow government organizations to handle the service demand without any interruptions, as technology support is scaled to a much higher level than in on premise environment.

c. Modernization and innovation of government ICT and delivery services

Possibility of leveraging modern technologies and framework in order to quickly and securely deploy government applications.

d. Improving public sector resilience and recovery capabilities during times of crisis

Cloud solutions increase government resilience to cyber security threats, as it offers stronger cyber security and privacy capabilities and protection.

e. Ensuring that public sector keep up with growing technology advancements.

Cloud solutions facilitate future-ready government infrastructure, as moving to the cloud enables government organizations to grow with the latest technologies, rather than relying on outdated technological platforms.

f. Collaboration among government organizations for greater efficiency and better service delivery.

Cloud solutions enable effective collaboration as government organizations are able to easily share resources across organizations, providing greater efficiency, productivity and creativity in delivering online services.

g. Long term operational continuity and faster service recovery

As a result of centralized data storage; management and backups, data retrieval and business recovery during times of disaster (e.g. natural disasters or other disruptive events), it becomes easier and more cost effective to continue with uninterrupted operations.

h. Efficient Deployment of Services

Reducing the amount of infrastructure required to be built and owned by government organizations reduces overall deployment times and shifts the focus from management of infrastructure to delivery of faster services. ICT facilities and services can be deployed, tested and maintained efficiently than managing own ICT facilities.

1.2 NEED

The shift from the traditional data storage mechanisms towards Cloud Computing Solutions requires attention on formulating appropriate guidelines to ensure security and data protection, whilst enabling secure data flows. This demands a 'Government Cloud Services Policy' to provide the direction for government organizations to obtain the benefits of Cloud Computing and Storage Solutions in a manner which would promote efficiency, accuracy, interoperability, and security of data handled by them.

1.3 PURPOSE AND SCOPE

The Ministry of Technology has been mandated by the Gazette No. 2202/25 dated November 20, 2020 with the responsibility to establish digital governance services by optimal use of information technology, towards the achievement of anticipated goals in line with the government policy statement, 'Vistas of Prosperity and Splendour'. The Information and Communication Technology Agency (ICTA) is recognized as the implementing agency, and entrusted with the responsibility to formulate the 'Government Cloud Policy' on behalf of the Government of Sri Lanka.

The policy aims to prioritize the procurement of cloud based information and communication technologies. This will apply to infrastructure, hardware, software, information security, licensing, storage, provision of data, as well as services like security, development, virtualization, databases or any kind of technology where a cloud solution is equivalent to other forms of technological solutions.

1.4 RATIONALE

As per the definition of the U.S. National Institute of Standards and Technology (NIST);

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models".

The policy is devised on the basis of the following key principles.

a. Government organizations should be encouraged towards the optimal usage of cloud services to achieve higher degree of efficiency and productivity.
b. Emerging technology developments should be explored in the achievement of the government's digital transformation efforts and ensure the availability of required resources for such achievement.
c. Cost of total solutions i.e. purchasing, setting up, running and maintaining information services in the public sector should be minimized.
d. Government organizations should be empowered to respond to citizens and businesses in a more effective, efficient and productive manner.
e. Resilience of digital government services should be improved thorough a more developed service continuity and disaster recovery framework.

This policy aims to drive greater acceptance of cloud services in the public sector by adopting a 'cloud-first' approach to promote better infrastructural investments and an efficient IT deployment in the public sector.

1.5 APPLICABILITY

The policy shall apply to all government organizations and officers.

2 POLICY PRINCIPLES, STATEMENTS AND GOALS

The following sections formulates the principles, statements and goals which direct government organizations on how to use cloud computing to achieve security and remain resilient in terms of facilitating services to the public.

2.1 SELECTION OF A CLOUD SERVICE PROVIDER

The selection of a suitable cloud service provider is the most important and also the difficult in the process. As per the presidential circular PS/GPA/Circular/01/2020 government organizations are expected to obtain optimal use of national level ICT infrastructure under the supervision of the Information and Communication Technology Agency (ICTA) of Sri Lanka. Accordingly, all government organizations should consider Lanka Government Cloud (LGC), developed by ICTA, as the first preference in cloud service deployment.

If any government organization is of the view that their cloud service requirements cannot be fully addressed through the LGC, they can opt for a third party cloud service provider with the formal consent and approval of the Information and Communication Technology Agency (ICTA) of Sri Lanka. In such an event government organizations should provide a valid justification in consideration of the availability of the following[2] with the cloud service provider, which are pivotal in making the right choice.

a. Understand how cloud provider offerings address the key requirements and criteria
b. Use planning and controls to mitigate security and compliance risks
c. A structured framework for acquiring cloud management platform tools
d. A sound understanding on the process and architecture options for the migration towards cloud services
e. Research critical features and capabilities

[2] https://www.gartner.com/smarterwithgartner/5-priorities-when-buying-and-deploying-cloud-offerings

2.2 LIFECYCLE OF A CLOUD SOLUTION

The creation of a cloud platform takes a long number of steps and dedicated time. The following can be identified as the steps involved or the lifecycle of cloud computing solutions.

a. Step 1: Define the Purpose

The first and foremost step is to define the purpose for which government organizations want to obtain cloud services. In order to achieve this step, it is of great importance to understand the requirement and what type of an application is required to run on the cloud. Next is to decide the type of cloud functionalities and services in public (LGC), private, or hybrid models.

b. Step 2: Define the Hardware

Deciding what type of hardware is required is the most thought after the process. Thus, a precise decision should be taken in this regard. It is necessary to choose the service that will provide the right support when capacity is resized to maintain the application running.

c. Step 3: Define the Cloud Resources

Every application must have a good amount of cloud resources (vCPU, RAM, Storage) where data or application processing can be done in a secure manner. Thus, any cloud resource requirement should be chosen based on the application architecture and user requirements of the government organization. Also there should be a mechanism to backup and ensure disaster recovery of data.

d. Step 4: Define the Network

Network is the medium that will deliver data to the end users. Hence, the network must be configured in a manner which is flawless so that the intruders cannot break into the network. At the same time, it is important to define the network facilitating secure delivery of data, videos, and applications with low latency and high transfer speed. LGN can be considered as a secured government dedicated wide area network.

e. Step 5: Define the Security

Security is an indispensable aspect of any application. It is a must to set-up security services which enable user authentication or access limitation to a certain set of users. Government organizations needs to evaluate and ensure that security aspects of the cloud service provider is on par with the expected level.

f. Step 6: Define the Management Process and Tools

Government organizations should have complete control over the required resources for the application to be hosted. It is a must to define management tools which facilitate monitoring of the cloud environment, resources used, and the customer application running on it.

g. Step 7: Testing

Testing is another important stage in the lifecycle of any application deployment. Errors can be figured out only through the testing process involved in it. During testing, the application must be verified using various developer tools where coding is built, tested, and deployed whilst assuring security, vulnerability assessment (VA), penetration testing (PT) and fail over scenarios.

h. Step 8: Analytics

Finally, analyze and visualize data using analytics services where data querying and extraction is possible. Once analyzing is completed, the application becomes ready for deployment. In terms of cloud resources, optimization can be achieved based on the actual utilization of the cloud resources by the deployed application.

2.3 CLOUD COMPUTING SERVICE AND DEPLOYMENT MODELS

a. The policy recognizes the following cloud based service models. Government organizations can opt to a preferred model in consideration of their requirements and needs.

1. Infrastructure as a Service (IaaS)

The most basic category of cloud computing services. It allows one to rent IT infrastructure i.e. servers and virtual machines (VMs), storage, networks, operating systems, from a cloud provider on a pay-as-you-go basis[3].

2. Software as a Service (SaaS)

Software as a service is a method for delivering software applications over the internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure, and handle any maintenance, like software upgrades and security patching. Users connect to the application over the internet, usually with a web browser on their phone, tablet, or PC[4].

Email, social media, and cloud file storage solutions (such as Dropbox or Box) are few examples of SaaS applications that are often used by people in their day-to-day lives.

[3] https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#cloud-computing-models
[4] https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#cloud-computing-models

3. Platform as a Service (PaaS)

Platform as a service refers to cloud computing services that supply an on-demand environment for developing, testing, delivering, and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development[5].

Examples of PaaS solutions include AWS Elastic Beanstalk, Google App Engine, Microsoft Windows Azure, and Red Hat OpenShift on IBM Cloud.

b. The policy recognizes the following deployment models for cloud services.

1. Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It is owned, managed, and operated by a third-party CSP, which exists on the premises of the cloud provider. Users can access the services and manage their account via a web browser.

2. Private Cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers such as business units. It may be owned, managed, and operated by the organization, a third party, or a combination of both parties, and it may exist on or off premises. A private cloud is one in which the services and infrastructure are maintained on a private network.

3. Hybrid Cloud

The cloud infrastructure is a combination of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by technology that enables data and application portability. A hybrid cloud provides greater flexibility, more deployment options, and helps to optimize existing infrastructure, security, and compliance

4. Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns such as mission, security requirements, policy, and compliance considerations etc. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or a combination of them, and it may exist on or off premises.

c. The policy recommends government organizations to opt to a ‘private’ cloud which has been dedicatedly built for the government.

[5] https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#cloud-computing-models

d. Other types of clouds are also available for deployment, in order to address the specific requirements of government organizations.

2.4 ADOPTION OF CLOUD SERVICES

a. All government organizations shall adopt cloud computing as the preferred ICT deployment strategy for new ICT services and also when transforming the existing government services to digital applications, except if;

- It can be shown that an alternative ICT deployment strategy meets special requirements of the government organization; or

- It can be shown that an alternative ICT deployment strategy is more cost effective from the perspective of Total Cost of Ownership (TCO) and demonstrates at least the same level of security assurance that a cloud solution offers; or

- The particular cloud service or technology required by the government organization, is not available with the government owned cloud.

b. The adoption of cloud services should be supported with a business case which is approved by the higher management of the organization. The business case must include;

- A summary of the intended cloud solution including the purpose and benefits of the same.
- Required application architecture, operating system, technology etc.
- An assessment of security risks and mitigation actions depending on the information sensitivity and classification
- A user manual explaining the operational framework and support functions (including responsibility matrix, SLAs, KPIs, processes, procedures etc.)

2.5 PROCUREMENT OF CLOUD SERVICES

a. At the time of procuring cloud services, government organizations should ensure that the selected cloud service satisfies the following conditions.

- Fit for the purpose
- Provides adequate risk management for information and ICT assets as defined by the relevant security principles, and
- Adheres to local legal, procurement and regulatory guidelines

b. Government organizations should be extra careful to avoid 'vendor lock-in' at the time of procuring cloud services and should ensure that sufficient flexibility is available for future migration between platforms.

c. An analysis must be conducted on the costs and benefits of moving towards a cloud service. Assessment must include value for money, fitness for purpose, a clearly defined business case (including benefits), total cost of ownership (TCO), asset impact, organizational impact, and technical environment impact.

d. Government organizations should ensure the availability of technical support, technical architecture, SLAs, maintenance, responsibility matrix, a technical account manager (TAM) etc. at the time of procuring cloud services.

2.6 MIGRATION OF APPLICATION/DATA TO CLOUD

2.6.1 PRE-MIGRATION

a. Government organizations should analyze their services, needs, technical requirements, and policy constraints in order to prepare for the migration to cloud environment.

b. Data has to be categorized by its sensitivity prior to moving to the cloud. Accordingly, government organizations should prepare a list of all on-premise systems, applications and software and assign a priority level for migration.

c. Government organizations should carefully analyze their IT portfolio and create a roadmap for cloud deployment and migration. The roadmap should prioritize services that have high expected value and high readiness to maximize the benefits received and minimize the risk.

d. A comprehensive set of test scenarios should be prepared for every system, application, software and process in the on-premise environment to monitor, ensure and confirm the success of the migration and operational efficiency in the cloud environment. The administrators of every system, software, application and process should take the lead in this task.

e. Government organizations should carefully examine and map all of the dependencies in the on-premise solution and make sure that same is retained or improved in the cloud environment.

2.6.2 MIGRATION OF THE APPLICATION OR DATA (AS PER THE PLAN)

a. The on-premise solution should also run in parallel during the cloud migration process, as a contingency plan, in order to avoid any impact to data.

b. Migration can take a piecemeal approach, where less sensitive data and on-premise solutions must be the initial focus, followed by others based on sensitivity.

c. Government organizations should ensure proper monitoring and validation during the migration process, in order to ensure the successful data migration to the cloud.

2.6.3 POST-MIGRATION

a. Conduct a post-migration validation, using the developed test scenarios, for each and every system, software, application and process in order to ensure that they are producing the same outcomes without disrupting normal operations.

b. Operational manuals, SLAs, governance structures, responsibility matrixes, and support and maintenance contracts should be updated accordingly in order to incorporate cloud migration related updates.

c. CDIO of each government organization should approve the migration plan confirming that all processes are fully migrated without any impact to the data and services and tested to ensure the functionality.

d. The availability of a comprehensive cloud migration plan (including pre/post-notifications required to update necessary stakeholder parties) to ensure a migration with lesser impact is mandatory.

2.7 DATA PROTECTION AND SECURITY

a. The cloud provider's policies should be compliant with the Sri Lankan legislation on data protection and security.

b. A periodic mapping of security threats and challenges to security compliances must be repeated and necessary updates made, for each system managed in the cloud, by the CSP in collaboration with the government organization.

c. A mapping of security threats and challenges to security capabilities must also be performed upon each security breach, incident and critical change affecting the cloud infrastructure.

d. The location of data is of prime importance. Thus high sensitive data and related copies/backup should remain within the legal boundaries of Sri Lanka to address data sovereignty concerns, whilst less sensitive data can be hosted in virtual locations outside Sri Lanka.

e. Develop cloud services based data privacy regulations and raise awareness on its importance among relevant staff.

f. The CSP should be compliant with widely adopted cloud security standards, as specified below, which are acceptable to the government.

- ISO/IEC 27017, demonstrated via certification with accreditation.
- NIST SP 800-53, demonstrated via certification with accreditation; or
- Level 2 of Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) Certification.

g. The CSP should provide a guarantee that the application, information and data provided by the government organization is stored in a secured environment that protects it from unauthorized access, modification, theft, misuse and destruction.

h. The CSP should maintain and enforce safety and physical security measures pertaining to access and maintenance of information. These measures should be;

- In par with industry standards
- In accordance with security requirements of the government organizations
- Able to provide appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access of information and all other data owned by a government organization and accessible by the CSP

i. Government organizations shall opt for a CSP with a Tier 3 certified Data Centre[6] that would accommodate the following.

- Multiple paths for power and cooling, and redundant systems that allow the staff to work on the set-up without taking it offline.
- No need of a total shutdown during maintenance or equipment replacement
- A back-up solution that can keep operations running in case of a local or region-wide power outage.
- Ensure that the equipment can continue to operate for at least 72 hours following an outage.

[6] https://phoenixnap.com/blog/data-center-tiers-classification

2.8 DISASTER RECOVERY, BACK-UP SERVICES AND SERVICE CONTINUITY

a. Apart from the main cloud services, government organizations can purchase disaster recovery and back-up services, which are considered as additional services.

- These are payable services
- Purchase of these services should be based on the criticality of the applications hosted in the cloud and related services

b. Government organizations needs to validate and ensure the ability of the selected CSP to perform the following to facilitate data recovery in a situation of emergency or disaster, as per the application criticality and service requirement.

- Ensure that it can make the services available even in the event of a disaster, power outage or similarly significant event.

- Maintain and implement disaster recovery and avoidance procedures to ensure that no solution is interrupted during any disaster. The CSP shall provide the government organization with a copy of its current disaster recovery plan and all updates thereto during the term.

- No government data loss occurs in the absence of data recovery mechanisms.

c. Government organizations need to ensure that the failure of one component of cloud services has less impact on overall service availability and reduces the risk of downtime.

d. Government organizations need to ensure that the disaster recovery solution is owned and managed entirely by the Contracted CSP.

2.9 CONNECTIVITY TO THE HOSTED SYSTEM

a. Every government organization is responsible to ensure the connectivity for the hosted system on the cloud via the internet.

b. If LGN connectivity is available at the government organization, same can be used as the network to connect to the LGC (if the application is hosted in the LGC).

c. Interruptions may occur due to slowness of internet connection and the government organization is responsible to ensure the reliability and efficiency of the connectivity speeds through the selected Internet Service Provider (ISP).

2.10 WORKFORCE READINESS

a. Government organizations should take appropriate measures to provide their staff with right skills and knowledge required for cloud hosting, migration and the subsequent use of cloud services.

b. Conduct a skill gap analysis, by every government organization, to map the current skills of the workforce against the required skills and develop strategies to address the identified gaps.

c. Chief Digital Information Officer (CDIOs) of every government organization must undertake the necessary workforce planning and provide necessary learning and developmental opportunities.

d. If a government organization has hired a 3rd party vendor for application development, hosting and service maintenance; same should be supported with a duly signed and valid agreement. And government organizations are responsible for maintaining continuity, updates and renewal of such agreement in accordance with their requirements.

2.11 DATA OWNERSHIP, RETRIEVAL AND INTEROPERABILITY

- Data Ownership

Government organizations must have the full control and ownership over their data, with proper measures to restrict access to customer infrastructure and data. CSP should provide a choice as to how they store, manage, and protect their data, and not require a long-term contract or exclusivity.

- Retrieval and Interoperability

Government organizations should be able to utilize common ICT infrastructure and facilities such as National Data Exchange (NDX), National Spatial Data Infrastructure (NSDI), Country Portal, Mobile Portal, GovSMS, Lanka Government Payment Service (to process electronic payments) and Government Information Centre (GIC, for citizen services for providing service related information to public) via interoperable cloud services, supporting collaboration and integrated government services.

2.12 SERVICE LEVEL AGREEMENTS (SLAs)

a. The provisioning of cloud solutions by CSPs to government organizations shall be governed by SLAs to specify and clarify performance expectations and establish accountability.

b. The SLAs should relate to the provisions in the contract pertaining to penalties, escalation procedures, disaster recovery, business continuity, and contract cancellation for the protection of the government organization in the event if the CSP failed to meet the required level of performance.

c. Government organizations should closely monitor the CSP's compliance with key SLA guidelines on the following aspects, among others;

- Availability and timeliness of services
- Confidentiality and integrity of data
- Change control
- Compliance to security standards
- Compliance to data protection including backups, retention periods, rights of the data subject and encryption controls; access management and data control permissions
- Business continuity including disaster recovery and contingency plans
- Right to change the CSP
- Help desk support
- Response time and resolution time

d. The roles and responsibilities of the government organizations, CSPs, and any other parties involved such as carriers etc. should be clearly explained and stated in the SLAs.

2.13 TERMINATION OF CLOUD SERVICES

a. Government organizations who opt for LGC services, should follow the termination process as specified in Section 3 on 'Term and Termination' of the agreement[7] entered into with the Information and Communication Technology Agency.

b. Government organizations who get partnered with third party CSPs are subject to the following.

- Government organizations should have the flexibility to terminate the cloud services/agreement at any time, upon a reasonable notice period (30 days) without subject to any penalty.

- In the event if a government organization moves to a new CSP, they need to assure that the existing CSP would provide necessary assistance required for such migration and proceed with the termination.

[7] Refer Annex 1 - Memorandum of Understanding for Utilizing Infrastructure Services of Lanka Government Cloud (LGC)

- In the event, if the CSP wants to terminate the services/agreement, for any reason, same should be informed to the government organization prior to 30 days.

- All government organizations shall instruct the CSP that the copies of data should be deleted, overwritten or otherwise made inaccessible upon expiration or termination of the contract.

- Upon the expiration or termination of the contract;

  - The CSP should provide, at no cost, a latest copy of all of the information in the form in use as of the date of such expiration or termination

  - The CSP should destroy or erase all other copies of the information, in the possession of the CSP or its agents or subcontractors, in any form including but not limited to electronic, hard copy or other memory device.

  - The government organization should obtain a certification in writing from the CSP, confirming that they have fully destroyed, erased or migrated all copies of the information and they shall not make any subsequent use of the information in a manner which would threaten its security.

  - Upon receiving the written confirmation from the CSP, the government organization should acknowledge the deletion of data or migration of data to a new cloud, as the case may be.

2.14 ADMINISTRATION AND ACCESS LEVELS

a. ICTA shall provide the tenant along with respective log-in credentials to the government organizations who would opt for LGC services.

- The government organization shall be the owner of the system within the dedicated resource pool allocated to the organization on LGC and the said resource pool is referred to as 'Tenant'.

- The responsibility of handling and maintaining the applications hosted in the allocated tenant, including the provision of access rights, solely lies with the government organizations.

b. Government organizations who obtain services from third party vendors or service providers should ensure;

- The existence of a valid agreement with the respective third party vendors or service providers having special focus on the confidentiality of data

- Access rights granted to third party service providers to access the cloud should be supported with a duly approved access authorization form

- Subsequent access rights granted, at different time intervals depending on organization requirements, should also get reflected in the same access authorization form.

2.15 SERVICE ASSURANCE OF THE CLOUD SERVICE PROVIDER

a. Government organizations who opt for LGC are provided with the assurances specified in the MoU[8] entered into with the Information and Communication Technology Agency of Sri Lanka.

- ICTA would perform an initial verification prior to providing the tenant i.e. cloud services, and assure that the software or applications expected to be hosted in LGC would perform in accordance to the guidelines and agreed specifications in the MoU.

b. In situations where a government organization gets partnered with a third party CSP, such CSP should be able to ensure the following.

- All services would be provided in a timely manner, in compliance with industry best practices.

- The CSP would provide a user guide/specification manual to the government organization on the use of the cloud services

c. The cloud services would comply with legal and legislative principles, rules and regulations in effect in Sri Lanka.

d. Data and information of the government organizations will not be shared with or disclosed in any manner to a third party by the CSP without prior written consent of the government organizations.

e. The cloud services would not infringe the intellectual property rights of any third party.

f. There is no pending litigation involving the CSP that may impair or interfere with the government organization's right to use the solution.

g. The CSP has sufficient authority to enter into an agreement and grant the rights provided in the agreement to the government organization.

[8] Refer Annex 1 - Memorandum of Understanding for Utilizing Infrastructure Services of Lanka Government Cloud (LGC)

3 CROSS BORDER DATA FLOWS

Cross border data flow possibilities for all government organizations are elaborated in the Part III of the Personal Data Protection Act, No. 9 of 2022[9], particularly by clause 26. All government organizations are advised strictly to follow these legal guidelines in deciding the locations to store their data in the cloud.

[9] https://www.icta.lk/icta-assets/uploads/2022/03/09-2022_E.pdf

4 LEGAL COMPLIANCE

The legal framework of Sri Lanka has introduced several enactments, as depicted below, embodying the key principles that are applicable to the policy context as well as the use of ICT services in government organizations.

a. Electronic Transactions Act No. 19 of 2006 as amended by Electronic Transactions (Amendment) Act No. 25 of 2017

b. Personal Data Protection Act No 19 of 2022

c. Computer Crimes Act No. 24 of 2007

All government organizations should adhere the applicable legal regulations in theses enactments and should ensure that the CSP is compliant to the same.

5 DATA CENTER USAGE

Depending upon the nature of the operation, some government organizations may think of having their own data centers, instead of using the cloud service facilities available. The policy of the government is not to encourage this practice given the high cost of setting up and maintaining data centers.

All government organizations, therefore, are advised to obtain the cloud facility of LGC as their first preference or any other suitable public/private/hybrid could facility depending upon their requirements.

This policy recognizes the important role played by the Information and Communication technology Agency in facilitating LGC services as well as other professional cloud services providers. It also guides the government organizations to let their cloud service provider run the backend of the solutions, while limiting their own roles to use the cloud facilities.

6 LANKA GOVERNMENT CLOUD (LGC)

ICTA has been mandated by the presidential circular No. PS/GPA/Circular/01/2020[10] to drive the national digital initiatives of the government. The circular entrusts ICTA with the responsibility to ensure the optimal use of national level ICT infrastructure under which LGC plays a pivotal role.

Lanka Government Cloud (LGC) is a government owned community cloud, managed by the Information and Communication Technology Agency of Sri Lanka, which has been implemented to provide cost effective, reliable and secure ICT infrastructure facilities to the public sector of the country, with the intention of achieving the following deliverables.

- Provide the citizens with convenient access to the government services
- Improved and efficient government services and electronic accessibility (as e-Services) for the same from anywhere and anytime
- Right to information
- Knowledge based society

Any government organization can use the LGC facilities upon entering into an agreement[11] with ICTA.

LGC can host central, web based and cloud ready government systems developed by the government organizations. Further, government organizations can utilize the centrally available software services provided by the LGC such as common HRM system, eRevenue License System, eLocal Government etc.

At present, LGC offers the following services.

- Back-up as a service
- Web Application Firewall (WAF)

[10] Refer Annex 2 – Presidential Circular No. PS/GPA/Circular/01/2020

[11] Refer Annex 1 - Memorandum of Understanding for Utilizing Infrastructure Services of Lanka Government Cloud (LGC)

7 POLICY IMPLEMENTATION

7.1 RESPONSIBILITY & AUTHORITY

7.1.1 GOVERNMENT ORGANIZATIONS

a. All government organizations involved in procuring cloud based services, applications or platform hosting services for the government organizations must adhere to this policy.

b. The CDIO of every government organization is responsible for ensuring the application and adherence to this policy within the organization.

c. Government organizations should take all efforts to minimize the usage and expansion of data centers, IT storage or processing infrastructure. Instead efforts should be taken to deploy cloud services as appropriate.

d. Appoint a dedicated cloud administration and support team, under the supervision of the CDIO, in order to address organizational transformation and subsequent operational efficacy.

e. Adhere to the guidelines, instructions for the use of cloud services prepared by the Ministry of Technology, and ensure that the staff apply these guidelines and instructions accordingly.

f. Government organizations are expected to cooperate with ICTA (for LGC) or the CSP (for third party cloud services) from time to time to perform essential infrastructure upgrades such as hardware, network infrastructure updates/upgrades and cloud platform upgrades/updates.

g. Government organizations are further expected to cooperate with ICTA (for LGC) or the CSP (for third party cloud solutions) in the event the cloud resources currently being provided would need to be migrated to a new cloud or platform to ensure scalability and adherence with new technology, security, and operational standards.

h. The government organizations shall not sign an agreement with a third party CSP prior to the completion and passing of all the mandatory controls in the CSP Assessment Questionnaire[12].

[12] Annex 4 – CSP Assessment Questionnaire

7.1.2 IMPLEMENTATION AGENCY

a. The implementation of the policy will be monitored and governed by the Information and Communication Technology Agency (ICTA) of Sri Lanka.

b. The implementation agency should ensure that the responsibilities enshrined in the MoU[13] between the government organizations and the implementation agency at the time of adopting LGC services are duly carried out, with the least impact to the client.

c. The implementation agency should work together with government organizations in order to strike a balance between client requirements, data privacy, data security and intellectual property of national data.

d. It is the responsibility of the implementation agency to ensure that this policy is evaluated at regular intervals in order to accommodate changes, as and when applicable, to uphold its effectiveness, timeliness and inclusiveness.

7.1.3 THIRD PARTY CLOUD SERVICE PROVIDERS

a. It is the responsibility of the CSP to protect its cloud system and maintain confidentiality, integrity and availability of its data.

b. Data shall not be stored, shared, processed, or modified in any manner which threatens its integrity.

c. CSPs should not have access to monitor their customers' data and content, thus strict adherence should be maintained to the required level of confidentiality by the government organizations.

d. CSPs should be able to provide necessary support to perform periodic audits or investigations as and when required by the government organizations and any legitimate government party.

e. The failure to satisfy any of the responsibilities on the part of the CSP shall constitute a breach of the contract.

    - The government organizations shall contractually state that the CSP will be held responsible for any financial losses or penalties (up to the agreed Cap or tolerance limit) that may occur due to a CSP breach.

[13] Refer Annex 1 - Memorandum of Understanding for Utilizing Infrastructure Services of Lanka Government Cloud (LGC)

- Identification of such a breach would necessitate the government organizations to terminate the contract with the CSP, subject to the stipulated timelines in the service contract.

f. It is the responsibility of the CSP to notify the government organization within 24 hours of a potential or actual breach or incident that may affect and threaten the organization's information hosted in the cloud.

g. CSPs must provide adequate investigative support to the government organizations.

h. CSPs should retain the investigation reports related to any security investigation for a period of 2 years upon the completion of the investigation progress.

i. CSPs must support e-discovery and legal holds to meet the needs of investigations and judicial requests.

7.2 MONITORING & EVALUATION

Monitoring and evaluation is an indispensable element which facilitates government organizations with an understanding of the progress and the achievement of intended outcomes of opting for cloud services. It further provides a base for timely planning of apt measures to address the identified issues and gaps.

Government organizations should conduct periodic monitoring and evaluation exercise in order to analyze the following.

a. Existence of security vulnerabilities which would threaten the confidentiality of data and performance of the applications hosted in the cloud.

b. Unauthorized deletion and modification of applications and data hosted in the cloud.

c. User experience in using cloud based applications. Monitor metrics such as response times and frequency of use to get the complete picture of performance.

d. Optimized resource utilization

   Evaluate the use of applications hosted in the cloud in order to identify the ones which are not getting frequently used in order to identify the

e. Monitor and troubleshoot of infrastructure

   Analyze the operational logs and metrics in near real time to identify trends and patterns in application performance and use the observations to reduce the mean time to repair (MTTR).

ANNEX 1 – FAQs

1. What is cloud computing?

Cloud computing is described as the process of using a network of remote servers, hosted via the internet, to store, manage and process data, rather than hosting it locally in an on premise environment. It is using someone else's (LGC or a third party cloud service provider) infrastructure and hardware, reducing the amount of capital investments you need to make.

2. What are the benefits that cloud services could bring to the organization?

The benefits of flexibility, scalability and cost savings are some of the key benefits that a government organization could largely earn.

It is equally important to evaluate if cloud is right for the organization from a strategic and operational perspective. This could be achieved by evaluating the current IT set-up to understand the benefits of moving to the cloud, especially in the following areas:

- Service
  How important are security, reliability and flexibility to the organization? Is the current solution meets the organizational needs? Is there room for improvement?

- Technology Landscape
  How many users are there? What is the geographic distribution of your user base? Do your employees require remote access?

- Cost
  Are you satisfied with the costs of your on premise solution? Are the costs to scale up or upgrade services acceptable?

- Ease of migration
  When was the last investment on capital expenditure? Is there any contractual and vendor commitments that constrain migration?

3. Why government organizations need to migrate to cloud services?

Maintaining on-premise services generally incurs a massive cost especially for storage and maintenance. Since the government is focused on a digital transformation in every domain, adoption of cloud services would provide government organizations with enhanced efficiency, agility and scalability at a lesser cost. Similarly, it would minimize the manual intervention involved in on-premise services where government organizations cold effectively utilize its human capital in a more productive manner to elevate operational and service excellence.

4. How to get prepared for cloud migration?

Preparing for cloud migration needs proper planning and analyzing at large. Government organizations needs to analyze the requirement of moving to a cloud and prioritize what data to be migrated first by way of having a migration plan. Another key aspect to consider is the network bandwidth and an organization may consider upgrading bandwidth or investing on increased connectivity in order to obtain the maximum use of cloud services.

5. What type of data/workload can be moved to the cloud?

The exercise of moving data to a cloud largely depends on the nature of the organization and its cloud strategy. An organization may choose to take a slow approach or a one-time approach in moving all of its data to the cloud. Further, some organizations use cloud services for data backup purposes as well. The ability to transform environments in a matter of minutes, scale them up or down on demand, and data accessibility from anywhere is a great benefit that cloud services facilitate.

6. Does the transition process needs new or additional staff?

Generally, the cloud service provider handles the transition process. Hence, there is very minimal need for new recruitments to proceed with it. However, having some IT expertise is helpful to make the transition smooth and also to coordinate with the cloud service provider as well as other services providers who host services/applications in the cloud.

7. What is the assurance on data accessibility?

The cloud provider would provide access, security, services and support upon partnering with them. Further, in order to ensure accessibility of data, cloud providers develop a service level agreement (SLA) which will detail what happens in the event of an outage and protects the customer in certain situations.

8. Why LGC?

LGC is the government cloud infrastructure which offers secure and reliable infrastructure facilities to the government to host any type of application or system. The implementation agency for LGC is ICTA who is committed to provide an uninterrupted technical assistance for the partnered government organizations.

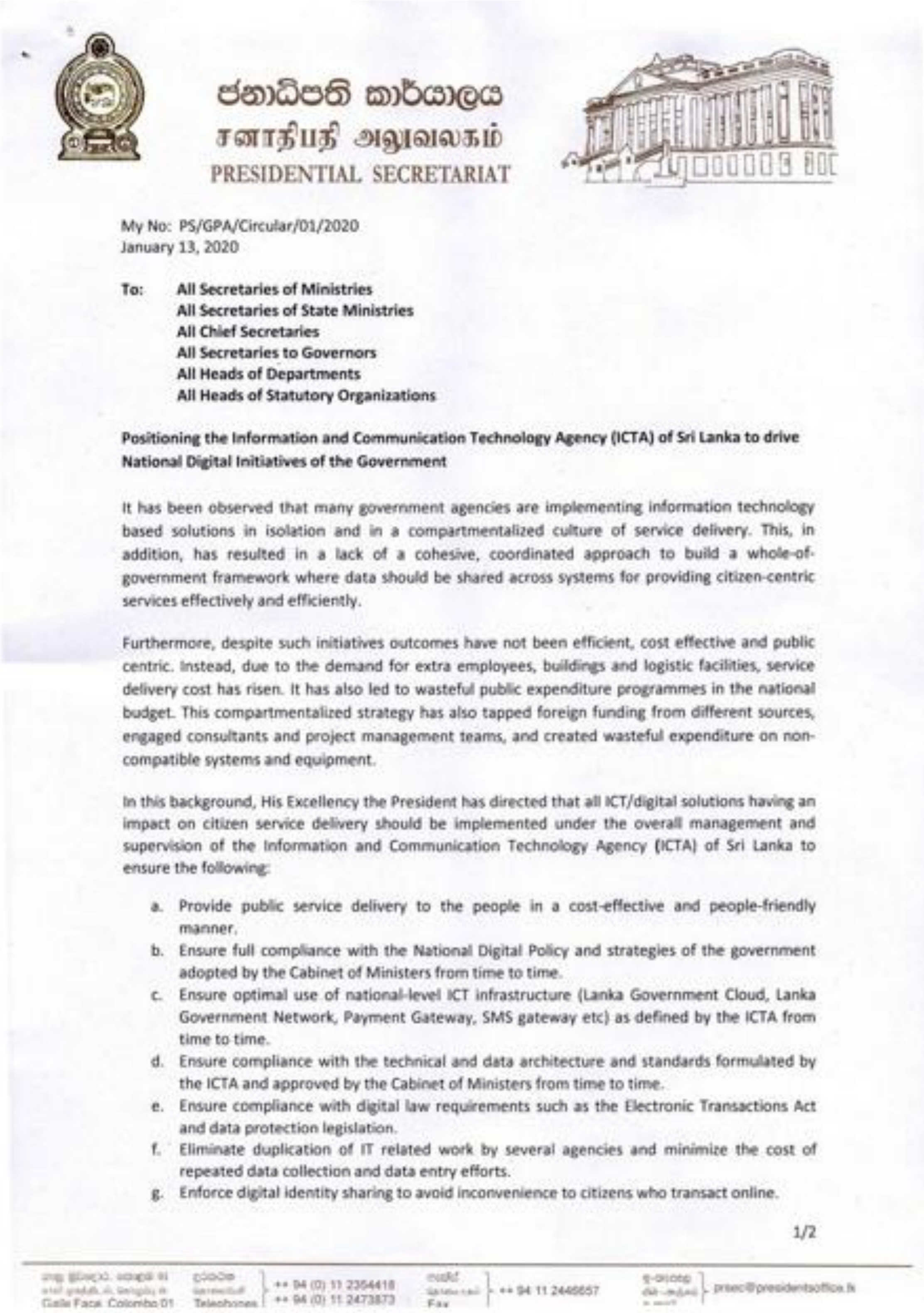
9. Is there a flexibility to opt for a third party cloud service provider, without LGC?

Yes, government organizations are free to decide whether to opt to LGC or any other third party cloud service provider. The decisive factor to consider is which option would best suit your needs.

ANNEX 2 – MEMORANDUM OF UNDERSTANDING FOR UTILIZING INFRASTRUCTURE SERVICES OF LANKA GOVERNMENT CLOUD (LGC)

ICTA-Letter-to-Govt
-Inst-LGC2-New-Mo

ANNEX 3 – PRESIDENTIAL CIRCULAR NO. PS/GPA/CIRCULAR/01/2020



ජනාධිපති කාර්යාලය
சனாதிபதி அலுவலகம்
PRESIDENTIAL SECRETARIAT

My No: PS/GPA/Circular/01/2020
January 13, 2020

To: **All Secretaries of Ministries**
All Secretaries of State Ministries
All Chief Secretaries
All Secretaries to Governors
All Heads of Departments
All Heads of Statutory Organizations

Positioning the Information and Communication Technology Agency (ICTA) of Sri Lanka to drive National Digital Initiatives of the Government

It has been observed that many government agencies are implementing information technology based solutions in isolation and in a compartmentalized culture of service delivery. This, in addition, has resulted in a lack of a cohesive, coordinated approach to build a whole-of-government framework where data should be shared across systems for providing citizen-centric services effectively and efficiently.

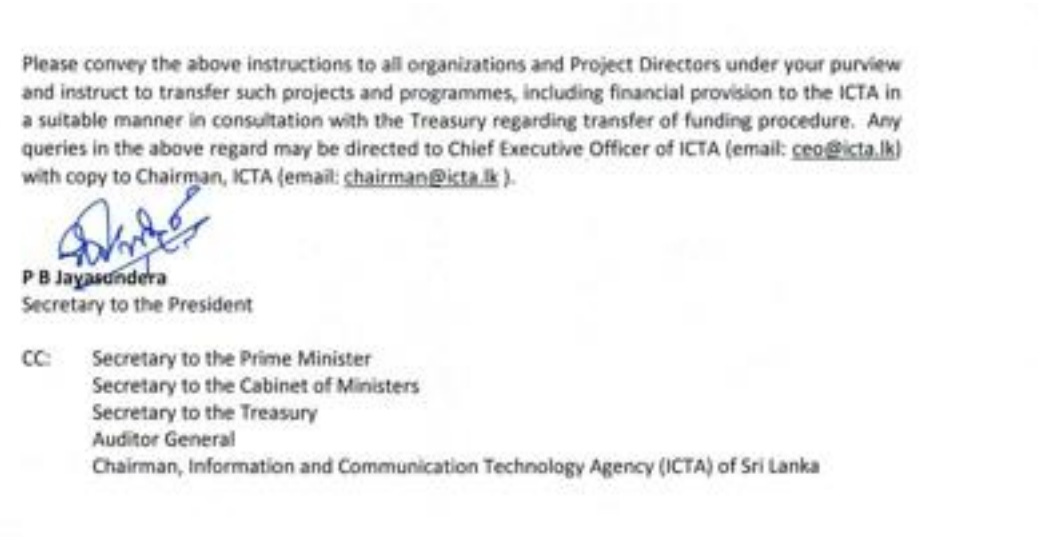
Furthermore, despite such initiatives outcomes have not been efficient, cost effective and public centric. Instead, due to the demand for extra employees, buildings and logistic facilities, service delivery cost has risen. It has also led to wasteful public expenditure programmes in the national budget. This compartmentalized strategy has also tapped foreign funding from different sources, engaged consultants and project management teams, and created wasteful expenditure on non-compatible systems and equipment.

In this background, His Excellency the President has directed that all ICT/digital solutions having an impact on citizen service delivery should be implemented under the overall management and supervision of the Information and Communication Technology Agency (ICTA) of Sri Lanka to ensure the following:

a. Provide public service delivery to the people in a cost-effective and people-friendly manner.
b. Ensure full compliance with the National Digital Policy and strategies of the government adopted by the Cabinet of Ministers from time to time.
c. Ensure optimal use of national-level ICT infrastructure (Lanka Government Cloud, Lanka Government Network, Payment Gateway, SMS gateway etc) as defined by the ICTA from time to time.
d. Ensure compliance with the technical and data architecture and standards formulated by the ICTA and approved by the Cabinet of Ministers from time to time.
e. Ensure compliance with digital law requirements such as the Electronic Transactions Act and data protection legislation.
f. Eliminate duplication of IT related work by several agencies and minimize the cost of repeated data collection and data entry efforts.
g. Enforce digital identity sharing to avoid inconvenience to citizens who transact online.

1/2

Galle Face, Colombo 01 Telephones ++ 94 (0) 11 2354418 ++ 94 (0) 11 2473873 Fax ++ 94 11 2446657 psec@presidentsoffice.lk



Please convey the above instructions to all organizations and Project Directors under your purview and instruct to transfer such projects and programmes, including financial provision to the ICTA in a suitable manner in consultation with the Treasury regarding transfer of funding procedure. Any queries in the above regard may be directed to Chief Executive Officer of ICTA (email: ceo@icta.lk) with copy to Chairman, ICTA (email: chairman@icta.lk).

P B Jayasundera
Secretary to the President

CC: Secretary to the Prime Minister
Secretary to the Cabinet of Ministers
Secretary to the Treasury
Auditor General
Chairman, Information and Communication Technology Agency (ICTA) of Sri Lanka

ANNEX 4 – CSP ASSESSMENT QUESTIONNAIRE

No	Control Domain	Assessment	Answer	Reference
1.	Independent Audits	Do you allow customers to view your third party audit reports?		
		Do you conduct network penetration tests of your cloud service infrastructure regularly? If yes please elaborate on your test and remediation process.		
		Do you conduct regular application penetration tests of your cloud infrastructure according to the industry best practices? If yes please elaborate on your test and remediation process.		
		Do you conduct internal audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.		
		Do you conduct external audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.		
		Are the results of the network penetration tests available to customers at their request?		
		Are the results of internal and external audits available to customers at their request?		
2.	Third Party Audits	Do you permit customers to perform independent vulnerability assessments?		
3.	Contact/Authority Maintenance	Do you maintain updated liaisons and points of contact with local authorities? If yes then how frequently you validate the contacts?		
4.	Information System Regulatory Mapping	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single customer only, without inadvertently accessing another customer's data?		
		Do you have capability to logically segment, isolate and recover data		

No	Control Domain	Assessment	Answer	Reference
		for a specific customer in the case of a failure or data loss?		
5.	Intellectual Property	Do you have policies and procedures in place describing what controls you have in place to protect customer's data marked as intellectual property?		
		If utilization of customers services housed in the cloud is mined for cloud provider benefit, are the customers' defined IP rights preserved?		
		If utilization of customers services housed in the cloud is mined for cloud provider benefit, do you provide customers the ability to optout?		
6.	Ownership	Do you follow or support a structured data-labelling standard (ex. ISO 15489, Oasis XML Catalogue Specification, CSA data type guidance)? If yes please specify		
7.	Classification	Do you provide a capability to identify virtual machines via policy tags/metadata?		
		Do you provide a capability to identify hardware via policy tags/metadata/hardware tags?		
		Do you have a capability to use system geographic location as an authentication factor?		
		Do you allow customers to define acceptable geographical locations for data routing or resource instantiation?		
8.	Handling / Labelling / Security Policy	Do you consider all customer data to be "highly sensitive "and provide the same protection and controls across the board or you apply the controls according to the data specific classification or label?		
		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data		

No	Control Domain	Assessment	Answer	Reference
9.	Retention Policy	Do you have technical control capabilities to enforce customer data retention policies?		
		Do you have a documented procedure for responding to requests for customer data from governments or third parties?		
10.	Secure Disposal	Do you support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the customer?		
		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of customer data once a customer has exited your environment or has vacated a resource?		
11.	Nonproduction Data	Do you have procedures in place to ensure production data shall not be replicated or used in your test environments?		
12.	Information Leakage	Do you have controls in place to prevent data leakage or intentional/accidental compromise between customers in a multi-customer environment?		
		Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?		
13.	Policy	Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?		
14.	User Access	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background checks?		
15.	Controlled Access Points	Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication		

No	Control Domain	Assessment	Answer	Reference
		mechanisms, reception desks and security patrols) implemented?		
16.	Secure Area Authorization	Do you allow customers to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?		
17.	Unauthorized Persons Entry	Are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises monitored, controlled and isolated from data storage and process?		
18.	Offsite Authorization	Do you provide customers with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business continuity failovers, replication)		
19.	Offsite equipment	Do you provide customers with documentation describing your policies and procedures governing asset management and repurposing of equipment?		
20.	Asset Management	Do you maintain a complete inventory of all of your critical assets?		
21.	Employment Agreements	Do you specifically train your employees regarding their role vs. the customer's role in providing information security controls?		
		Do you document employee acknowledgment of training they have completed?		
22.	Employment Termination	Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?		
23.	Management Program	Do you provide customers with documentation describing your Information Security Management System (ISMS)?		

No	Control Domain	Assessment	Answer	Reference
24.	Management Support / Involvement	Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?		
25.	IS Policy	Do your information security and privacy policies align with particular standards (ISO27001, NIA, CoBIT, etc.)?		
		Do you have agreements which ensure your providers adhere to your information security and privacy policies?		
		Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?		
26.	Baseline Requirements	Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?		
		Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?		
		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?		
27.	Policy Reviews	Do you notify your customers when you make material changes to your information security and/or privacy policies?		
28.	Policy Enforcement	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?		
		Are employees made aware of what action might be taken in the event		

No	Control Domain	Assessment	Answer	Reference
		of a violation and stated as such in the policies and procedures?		
29.	User Access Policy	Do you have controls in place ensuring timely removal of access rights and permissions which is no longer required?		
		Do you provide metrics which track the speed with which you are able to remove access rights following a request from us?		
30.	User Access Restriction / Authorization	Do you document how you grant and approve access to customer data?		
		Do you have a method of aligning provider and customer data classification methodologies for access control purposes?		
31.	User Access Revocation	Is timely de-provisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties?		
32.	User Access Reviews	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your customers)?		
		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?		
		Will you share user entitlement remediation and certification reports with your customers, if inappropriate access may have been allowed to customer data?		
33.	Training/ Awareness	Do you provide or make available a formal security awareness training program for cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to customer data?		

No	Control Domain	Assessment	Answer	Reference
		Are administrators properly educated on their legal responsibilities with regard to security and data integrity?		
34.	Industry Knowledge/ Benchmarking	Do you participate in industry groups and professional associations related to information security?		
		Do you benchmark your security controls against industry standards?		
35.	Roles / Responsibilities	Do you provide customers with a role definition document clarifying your administrative responsibilities vs. those of the customer?		
36.	Management Oversight	Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?		
37.	Segregation of Duties	Do you provide customers with documentation on how you maintain segregation of duties within your cloud service offering?		
38.	User Responsibility	Is your staff made aware of their responsibilities for maintaining awareness and compliance with our published security policies, procedures, standards and applicable regulatory requirements?		
		Are users made aware of their responsibilities for maintaining a safe and secure working environment?		
		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?		
39.	Workspace	Do your data management policies and procedures address customer and service level security requirements?		
		Do your data management policies and procedures include a tamper audit or software integrity function		

No	Control Domain	Assessment	Answer	Reference
		for unauthorized access to customer data?		
		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?		
40.	Encryption	Do you have a capability to allow creation of unique encryption keys per customer?		
		Do you support customer generated encryption keys or permit customers to encrypt data to an identity without access to a public key certificate. (e.g. Identity based encryption)?		
41.	Encryption Key Management	Do you encrypt customer data at rest (on disk/storage) within your environment?		
		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?		
		Do you have a capability to manage encryption keys on behalf of customers?		
		Do you maintain key management procedures?		
42.	Vulnerability / Patch Management	Do you conduct network layer vulnerability scans regularly?		
		Do you conduct application layer vulnerability scans regularly?		
		Do you conduct local operating system-layer vulnerability scans regularly?		
		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?		
		Will you provide your risk based systems patching timeframes to your customers upon request?		
43.	Antivirus / Malicious Software	Do you deploy multi antimalware engines in your infrastructure?		
		Do you ensure that security threat detection systems which use		

No	Control Domain	Assessment	Answer	Reference
		signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?		
44.	Incident Management	Do you have a documented security incident response plan?		
		Do you integrate customized customer requirements into your security incident response plans?		
		Do you have a CERT function (Computer Emergency Response Team)?		
		Do you publish a roles and responsibilities document specifying what you vs. your customers are responsible for during security incidents?		
45.	Incident Reporting	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?		
		Does your logging and monitoring framework allow isolation of an incident to specific customers?		
46.	Incident Response Legal Preparation	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?		
		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?		
		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific customer without freezing other customer data?		
		Do you enforce and attest to customer data separation when producing data in response to legal subpoenas?		
47.	Acceptable Use	Do you provide documentation regarding how you may utilize or access customer data and/or metadata?		

No	Control Domain	Assessment	Answer	Reference
		Do you collect or create metadata about customer data usage through the use of inspection technologies (search engines, etc.)?		
		Do you allow customers to optout of having their data/metadata accessed via inspection technologies?		
48.	Asset Returns	Are systems in place to monitor for privacy breaches and notify customers expeditiously if a privacy event may have impacted their data?		
		Is your Privacy Policy aligned with industry standards and Sri Lankan's Law		
49.	e-Commerce Transactions	Do you provide standard encryption methodologies (3DES, AES, etc.) to customers in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)		
		Do you utilize standard encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?		
50.	Audit Tools Access	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)		
51.	Source Code Access Restriction	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?		
		Are controls in place to prevent unauthorized access to customer application, program or object source code, and assure it is restricted to authorized personnel only?		

No	Control Domain	Assessment	Answer	Reference
52.	Nondisclosure Agreements	Are requirements for nondisclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?		
53.	Third Party Agreements	Can you provide a list of current 3rd party organization that will have access to the customer's (My) data?		
54.	Equipment Maintenance	If using virtual infrastructure, does your cloud solution include hardware independent restore and recovery capabilities including offsite storage of backups?		
		If using virtual infrastructure, do you provide customers with a capability to restore a Virtual Machine to a previous state in time?		
		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		
		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?		
		Do you share reports on your backup/recovery exercise results?		
		Does your cloud solution include software / provider independent restore and recovery capabilities?		
55.	Assessments	Are formal risk assessments aligned with the enterprise wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?		
		s the likelihood and impact associated with inherent and residual risk determined independently, considering all risk		

No	Control Domain	Assessment	Answer	Reference
		categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?		
56.	Mitigation / Acceptance	Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?		
		Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?		
57.	Business / Policy Change Impacts	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?		
58.	Third Party Access	Do you monitor service continuity with upstream internet providers in the event of provider failure?		
		Do you have more than one provider for each service you depend on?		
		Do you provide access to operational redundancy and continuity summaries which include the services on which you depend?		
		Do you provide the customer the ability to declare a disaster?		
		Do you provide a customer triggered failover option?		
		Do you share your business continuity and redundancy plans with your customers?		
59.	New Development / Acquisition	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?		
60.	Production Changes	Do you provide customers with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?		

No	Control Domain	Assessment	Answer	Reference
61.	Quality Testing	Do you have controls in place to ensure that standards of quality are being met for all software development?		
		Do you have controls in place to detect source code security defects for any outsourced software development activities?		
62.	Unauthorized Software Installations	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?		
63.	Impact Analysis	Do you provide customers with on-going visibility and reporting into your operational Service Level Agreement (SLA) performance?		
		Do you provide customers with on-going visibility and reporting into your SLA performance?		
64.	Business Continuity Planning	Are you BS25999 or ISO 22301 certified?		
		Do you provide customers with geographically resilient hosting options?		
65.	Business Continuity Testing	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?		
66.	Environmental Risks	Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?		
67.	Equipment Power Failures	Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?		
68.	Power / Telecommunications	Do you provide customers with documentation showing the transport route of their data between your systems?		
		Can customers define how their data is transported and through which legal jurisdiction?		

No	Control Domain	Assessment	Answer	Reference
69.	Customer Access Requirements	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?		
		Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a customer) if requested?		
		Do you provide customers with strong (multifactor) authentication options (digital certs, tokens, biometric, etc...) for user access?		
		Do you allow customers to use third party identity assurance services?		
		Do you utilize an automated source-code analysis tool to detect code security defects prior to production?		
		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?		
70.	Data Integrity	For your PaaS offering, do you provide customers with separate environments for production and test processes?		
		For your IaaS offering, do you provide customers with guidance on how to create suitable production and test environments?		
71.	Audit Logging / Intrusion Detection	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?		
		Is Physical and logical user access to audit logs restricted to authorized personnel?		
		Can you provide evidence that due diligence mapping of currently		

No	Control Domain	Assessment	Answer	Reference
		applicable regulations and standards to your controls/architecture/process es has been done?		

REFERENCES

- https://www.gartner.com/smarterwithgartner/5-priorities-when-buying-and-deploying-cloud-offerings
- https://www.slideshare.net/wasanthadesha/lanka-government-cloud-what-why-how
- https://aws.amazon.com/cloudwatch/