DRAFT VERSION. PLS DO NOT QUOTE

POLICY/GUIDELINE FOR THE ADOPTION OF CLOUD SERVICES BY GOVERNMENT ORGANIZATIONS IN SRI LANKA

DRAFT V 1.12

INFORMATION AND COMMUNICATION TECHNOLOGY AGENCY OF SRI LANKA

ICTA
ideas actioned
Information and Communication Technology Agency

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 Information Security Team
1.8	07.11.2023	Revisit by the Data Infrastructure and Data Services Thematic Working Group
1.9	23.11.2023	Review 1 – ICTA CXOs/Directors
1.10	31.01.2024	Review with Senior Manager – Network and Infrastructure Solutions
1.11	06.02.2024	Review 2 – ICTA CXOs/Directors
1.12	12.02.2024	Review 3 – ICTA CXOs/Directors

LIST OF ABBREVIATIONS

CSP	Cloud Service Provider
FoC	Free of Charge
GoSL	Government of Sri Lanka
IaaS	Infrastructure as a Service
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

LIST OF TABLES

LIST OF FIGURES

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.

1.2 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 'Cloud Adoption Policy/Guideline for Government' 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 policy/guideline aims to prioritize the procurement of cloud based ICTs and promote widespread adoption of cloud services by Government organizations as part of their IT investment decision-making process.

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 aspects.

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.

The 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.

2 THE NEED FOR A 'CLOUD FIRST' APPROACH

The Government of Sri Lanka strongly advocates for a 'Cloud First' strategy when government organizations require hosting services. Accordingly, all government organizations shall adopt cloud service as the preferred strategy for new ICT service deployment and also when transforming the existing services to digital applications, except if it can be shown that an alternative ICT deployment strategy;

- Meets special requirements of the government organization or
- More cost effective from the perspective of Total Cost of Ownership (TCO)[1] or
- Demonstrates 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 in the government owned cloud i.e. Lanka Government Cloud.

Alternative solutions, such as on-premises solutions, can only be explored as a last resort if a cloud-based solution is not practical. This is the recommended approach to the entire public sector, unless organizational specific circumstances stand as a hindrance.

[1] Refer Annex 1 – Total Cost of Ownership

3 PRINCIPLES TO FOLLOW

The selection of a suitable cloud service provider (CSP) constitutes a fundamental decision in a successful cloud migration journey undertaken by a government organization. Adherence to a defined set of principles, would drive organizations towards informed decisions throughout the migration journey, maximizing the RoI.

Government organizations should prioritize the eight (8) principles outlined in this section, when choosing a CSP. These principles act as essential safeguards to ensure that the most suitable CSP, who could deliver optimal outcomes, is chosen.

Principle	Factors to Consider
Data Security	Selecting the right CSP involves carefully consideration of various security factors to ensure your data and systems remain protected. Here are some key aspects to consider: ▪ Data Security: Encryption, Access Controls, Identity and Access Management (IAM), Data Loss Prevention (DLP) etc. ▪ Security Infrastructure and Practices: Security certifications, Threat detection and prevention, Incident response, Physical security, Vulnerability management etc.
Data Sovereignty	CSP's compliance with Sri Lankan laws and regulations, especially the Personal Data Protection Act No. 9 or 2022[2]. The policy recommends simultaneous focus on the aspects of data localization and storage as well as data access and control in order to ensure optimal benefits[3].
Cost Optimization	Conduct a thorough cost-benefit analysis considering upfront migration costs, ongoing subscription fees, data transfer costs and potential cost savings from resource optimization. Cost optimization is an ongoing process, which requires continuous monitoring, analyzing, and shaping the strategic approach as your cloud usage evolves.
Sustainability	Flexible pricing models that align with the organization's needs and avoid vendor lock-in
Transparency and Accountability	Continuous communication and open dialogue are critical for navigating the complexities of cloud migration and building a long-term, trusted relationship with your chosen CSP.

[2] Refer Annex 2 : Sri Lanka's Legal Landscape on Cross Border Data Flow
[3] Refer Annex 3 : Data Sovereignty and Data Localization

Principle	Factors to Consider
	Following are some key areas for consideration which bring transparency and accountability. ▪ **Migration Transparency:** A clearly defined migration plan, regular communication and access to migration logs and reports. ▪ **Data Transparency** ▪ **Security Transparency:** Security compliance certifications, security audits and reports and incident response ▪ **Performance Transparency:** Monitoring and reporting tools, Service Level Agreements (SLAs) and Proactive communication. ▪ **Cost Transparency:** Clear pricing structure and cost optimization tools
Operational Efficiency	Seamless integration with existing IT infrastructure ensuring flexibility to accommodate scalability, resource optimization and automation.
Scalability	Scalability is a fundamental principle of cloud migration, allowing resources to be easily adjusted up or down based on demand. Key focus areas for evaluation are; ▪ Resource Elasticity ▪ Cost Optimization ▪ Enhanced Performance ▪ Load Balancing
Disaster Recovery and Business Continuity	Availability of disaster recovery and business continuity plans to minimize downtime and data loss in case of an outage, with a special focus on the following. ▪ Risk Assessment ▪ Reliable backup and replication solutions ▪ High availability architecture for critical applications

Table 1 : Cloud Migration Principles to Follow

The policy prioritizes the principle of 'Data Security', urging government organizations to make it their primary consideration.

4 CLOUD MIGRATION PROCESS

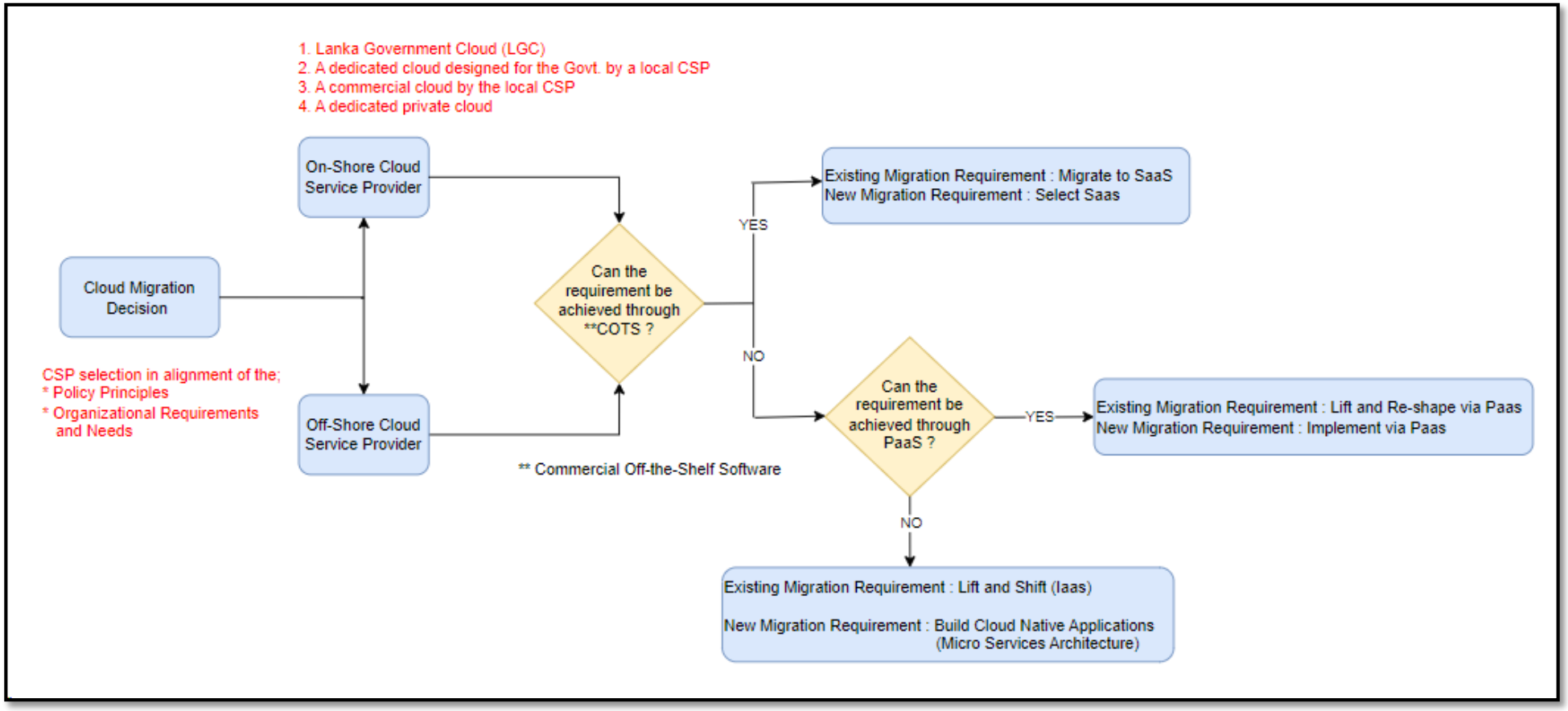

Figure 1: Cloud Migration Process - Decision Making Flow

4.1 Deciding the CSP: On-Shore or Off-Shore CSP

a. Determining the type of the CSP i.e. on-shore or off-shore CSP, is the very first decision making in the journey, setting the stage for subsequent decisions.

   - CSP selection should comply with the policy principles outlined in Section 3 above.

   - The on-shore / off-shore decision making necessitates careful consideration of data security and data sovereignty implications, in the light of Sri Lankan legal and regulatory landscape[4].

b. Government organizations with an 'On-Shore' CSP preference can evaluate potential providers in alignment of the following order, based on their adherence to the defined policy principles.

   1. Lanka Government Cloud (LGC)
   2. A dedicated cloud designed for the Government by a local CSP
   3. A commercial cloud by a local CSP
   4. A dedicated Private Cloud

c. Following the selection of the CSP, the next step is to determine the nature of the workload being migrated i.e. a new requirement or an existing requirement.

4.1.1 Migration of Existing Requirement

a. When considering cloud migration for existing requirements, government organizations should assess whether a Commercial Off-the-Shelf Solution (COTS) can fully address the requirement. If same is viable, opting to Software-as-a-Service (SaaS) model would be the best fit to achieve optimal benefits.

b. In the absence of a fully complete SaaS solution, the feasibility of re-platforming specific workloads in a Platform-as-a-Service (PaaS) model within the cloud infrastructure should be evaluated as a next step.

c. If Platform-as-a-Service (PaaS) model does not fully meet the requirements, government organizations can opt for Infrastructure-as-a-Service (IaaS) model as a viable alternative. This allows seamless migration of existing on-premises solutions to the cloud, preserving their functionality while leveraging the benefits of cloud infrastructure.

[4] Government organizations can seek advice from the Data Protection Authority in deciding the extent of applicability of the PDPA.

4.1.2 Migration of New Requirement

a. In terms of migrating a new requirement to cloud environment, same process from (a) to (b) as discussed in section 4.1.1 would follow.

b. Only difference is that in a new requirement, if PaaS model would not address the need; the most viable option is to build cloud native applications.

4.2 Deciding the components to migrate

When deciding which components to migrate, it is advisable to carry-out a pre-migration assessment[5] of the systems, platforms, solutions and applications that are used by the organization and decide which are to be retired, retained and migrated.

This assessment enables government organizations to ensure a seamless transition and achieve optimal benefits.

Type	Definition
Retire	Applications, systems, platforms or solutions which are of **no value to the organization and hardly used** by the organization.
Retain	Applications, systems, platforms or solutions which are **not cloud ready** thus, organization can retain them leaving as on-premises solutions.
Migrate	Applications, systems, platforms or solutions that the organization **decides to be moved** to a cloud environment.

Table 2 : Categorization of Migration Components

4.3 Migration Options

4.3.1 On-premises to Cloud Migration

Migration of on-premises solutions to a cloud environment. Following the comprehensive pre-migration assessment, government organizations can formulate a strategic cloud migration roadmap. This roadmap should prioritize the transfer of applications, systems, platforms, or solutions with minimal operational disruption, gradually ascending to ones with higher impact. This ensures minimal disruption to the ongoing workflows and fosters a smooth transition to the cloud environment.

4.3.2 Cloud to Cloud Migration

Migration of applications already hosted in a cloud platform to a different cloud platform.

[5] Refer Annex 4 : Cloud Adoption Lifecycle

4.3.3 On-premises to the Cloud Platform facilitated by the same vendor

Government organizations upon performing the pre-migration assessment can opt to migrating existing on-premises solutions to its cloud version provided by the same vendor.

5 A COMPARISON OF CLOUD MIGRATION APPROACHES

The choice of a cloud service provider depends on the specific needs and priorities of each government organization. Factors to consider include security requirements, compliance mandates, performance demands, budget constraints, and existing IT infrastructure. Carefully evaluating these factors and aligning them with the strengths of each cloud provider will lead to a well-informed decision that supports the organization's mission and objectives.

Government organizations are encouraged to select either of the following options that best aligns with their unique needs and the policy principles.

1. Lanka Government Cloud (LGC)
2. Commercial Cloud in Sri Lanka
3. Off-shore Cloud

This table offers a comparative analysis of different CSP options available to Government organizations. It aims to facilitate the selection of the most appropriate CSP based on the recognized policy principles.

Principle	LGC	Local CSP	International CSP
Data Security	Provides complete security protection for the infrastructure. In addition, client will be responsible for applying security precautions for the applications hosted in LGC.	Alignment with these principles may vary significantly between different CSPs. In order to ensure optimal alignment with the policy principles, government organizations are advised to carefully evaluate and select the CSP that best serves the same.	Alignment with these principles may vary significantly between different CSPs. In order to ensure optimal alignment with the policy principles, government organizations are advised to carefully evaluate and select the CSP that best serves the same.
Data Sovereignty	Data sovereignty aspects are fully guaranteed in alignment with Sri Lankan legal and regulatory landscape.		
Cost Optimization	Currently, offered on Free of Charge (FoC) basis. Planning to implement Pay-as-you-go model in the next version.		
Sustainability	This project is owned by GoSL and currently operated by ICTA thus, sustainability is guaranteed.		
Transparency and Accountability	This project is owned by GoSL and currently operated by ICTA thus, transparency and accountability are guaranteed.		
Operational Efficiency	Application or data can be accessed from anywhere supported with LGN or public internet connectivity.		
Scalability	Flexibility exists to upscale/ downscale resources based on the client request.		
Disaster Recovery and Business Continuity	Strong contract with principle service providers including local support and delegated Technical Account Manager (TAM). In addition, certified LGC support technical team involved in day-today operations provide NoC operations.		

Table 3: Comparison of Different Cloud Adoption Options

6 DATA OWNERSHIP, RETRIEVAL AND INTEROPERABILITY

6.1 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.

6.2 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.

7 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.

8 TERMINATION OF CLOUD SERVICES

a. 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.

b. 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.

c. 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.

d. 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.

e. 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.

9 ADMINISTRATION AND ACCESS LEVELS

a. The existence of a valid agreement with a special focus on the confidentiality of data

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

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

10 POLICY IMPLEMENTATION RESPONSIBILITY

10.1 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 coordinate with the CSP 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 coordinate with the CSP 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 specified in the CSP Assessment Questionnaire[6].

10.2 Cloud Service Provider

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.

[6] Refer Annex 5 : CSP Assessment Questionnaire

c. CSP 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. CSP 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.

f. 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.

g. 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.

h. 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.

i. CSP must provide adequate investigative support to the government organizations.

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

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