Government of the Republic of Trinidad and Tobago

Ministry of Public Administration

CLOUD COMPUTING CONSIDERATION POLICY

MARCH 2020

List of Abbreviations

CRM	Customer Relationship Management
CSPII	Confidential, Secret, Personally Identifiable Information
CSP	Cloud Service Provider
DLP	Data Loss Prevention
e-GIF	e-Government Interoperability Framework
e-GOTS	e-Government Omnibus Technical Standards
GoRTT	Government of the Republic of Trinidad & Tobago
GOVCLOUD	Government Cloud Computing
GOVNETT	Government ICT Network
GOVNETT NG	Digital Government Next Generation ICT Shared Services
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
iGOVTT	National Information and Communication Technology Company Limited
ISO	International Organization for Standardization
IPR	Intellectual Property Rights
IT	Information Technology
MDA	Ministries, Departments and Agencies
MPA	Ministry of Public Administration
NCA	Native Cloud Application
NIST	National Institute of Standards & Technology
OSD	Official Sensitive Data
PaaS	Platform as a Service
PII	Personally Identifiable Information
PSIP	Public Sector Investment Programme
SaaS	Software as a Service
SLA	Service Level Agreement
TCO	Total Cost of Ownership including initial acquisition cost, maintenance and operations costs
TTCSIRT	Trinidad and Tobago Computer Security Incident Response Team
UD	Unrestricted Data
Vision 2030	Trinidad and Tobago National Development Strategy, 2016-2030
WAN	Wide Area Network

WoG	Whole of Government

Table of Contents

Terminology

Cloud First – A cloud first approach involves the default delivery of ICT products and services from a cloud-based infrastructure rather than from an on-premise, private infrastructure owned by the Government Ministry, Department or Agency (MDA). In this approach, various cloud computing solutions are considered first and are preferred. Non-cloud delivered services are considered only if a cloud solution is deemed not to be feasible.

Consider Cloud – A consider cloud approach involves the inclusion of cloud delivered services as options that must be considered in the choice set and evaluation process for the acquisition of ICT solutions. It does not prescribe cloud delivered services and solutions as the only acceptable, default option.

Cloud Native – A native cloud approach involves the design, deployment and operations of applications and service processes specifically for delivery and support via various cloud computing architecture.

Cloud Computing – (also called simply, “the cloud”) describes the act of storing, managing and processing data online — as opposed to the organisation’s own physical computer or network.

- Since the Cloud is a broad collection of services, organisations can choose where, when, and how they use Cloud Computing.

- Cloud Computing is a general term that sits over a variety of services from Infrastructure as a Service (**IaaS**) at the base, through Platform as a Service (**PaaS**) as a development tool and through to Software as a Service (**SaaS**) replacing on premise software applications.

1. Introduction

Trinidad and Tobago is a small, twin island nation that must be competitive in an increasingly digitally connected global environment, where technological changes are rapidly unfolding. These changes introduce opportunities as well as new risks, challenges and complexities. It is incumbent on a forward thinking Government to create the necessary policies to leverage the benefits of developments in technology to improve the lives of all citizens.

Like many of its global counterparts, the Government of the Republic of Trinidad and Tobago (GoRTT) is faced with growing demands for greater accountability, improved public service delivery and faster implementation of appropriate, citizen-focused public sector programmes. In order for these demands to be met, the public service must become agile, responsive and cost efficient.

2. Background

Over the past two decades, significant investments have been made in public sector computerisation and digitisation. In moving forward, it is important to acknowledge and build upon this progress.

One of the five (5) themes of GoRTT's National Development Strategy for 2016 – 2030, Vision 2030, is *"Promoting Good Governance and Service Excellence"*[1]. The National ICT Plan 2018 - 2022 is in alignment with this theme. The Plan's Strategic Thrust 3: Enhancing Public Service Delivery, speaks to "ensuring the use of Information and Communication Technology (ICT) to achieve institutional strengthening and transformation of the delivery of public goods and services"[2]. The provision of secure, reliable, cost effective ICT solutions is a potent instrument of good governance. Relevant national ICT investments can foster greater collaboration, innovation and improved productivity in the public sector.

Globally, cloud computing has emerged as a major paradigm shift in the economics of acquiring, accessing, scaling and managing ICTs. The traditional capital expenditure intensive model of Governments being the owners of ICT assets is being superseded by cloud computing. Cloud computing supports a usage based, shared services consumption model. The antecedents to the adoption of Cloud Computing in Trinidad and Tobago is outlined in ***Appendix I*****.**

[1] National Development Strategy 2016-2030 (Vision 2030) p.48

[2] National ICT Plan 2018 to 2022: Cabinet Approved 13th August, 2018

The promise and the risks of cloud computing must be clearly identified, understood and appropriately managed. Thus, the strong interest, within the national community of information technology practitioners in the wider use of cloud platforms in the public sector, must be balanced with the necessary due diligence.

GoRTT has identified the wider adoption of cloud computing as a key mechanism for maximising returns on ICT investments to support enhanced delivery of public services. A critical success factor in this regard is the consideration to be given by Ministries, Departments and Agencies (MDAs) for the use of cloud based solutions which are secure, fit for purpose, comply with existing legislation and provide value for money as defined by the Public Procurement and Disposal of Public Property Act, 2015[3]. This policy fully acknowledges the Government's obligation to protect the data and privacy of all citizens.

3. Purpose

The purpose of the GoRTT CLOUD COMPUTING CONSIDERATION POLICY (the Policy) is to provide the requisite clarity, guidance and encouragement for the wider adoption of cloud services by MDAs. The Policy provides guidance for the use of cloud computing resources in a responsible and structured manner that will ensure the security of Government and citizen data.

4. Statement

Trinidad and Tobago's Government MDAs will:

- evaluate cloud services for new ICT solutions. In cases where the transition of current non-cloud operational services represent the best value for money, MDAs will choose cloud services where such services represent the best value for money, are compliant with data legislation and provide adequate management of risk compared to other available options;

- commence procurement of Cloud Services, as appropriate, for their testing and development needs where the service represents the best value for money and is fit for purpose; and

[3] The Public Procurement and Disposal of Public Property Act, 2015
http://www.ttparliament.org/legislations/a2015-01.pdf

- establish information sharing initiatives on adoption of cloud delivered services such as a repository of case studies, best practices and practical lessons to enable MDAs to learn from the experiences of innovators and early adopters. This will also seek to strike the requisite balance between trying many services to see what is most suitable and combining expenditure with fewer suppliers to leverage better discounts.

5. Principles

The following principles outline GoRTT's priorities in its adoption of cloud services.

- ✓ ***Cloud delivered services consumption costs be fully understood*** – Personnel at MDAs are to be trained in planning, consuming and leveraging cloud services that enable the achievement of public sector mandates. Cloud delivered service costs are fully understood and payments are based on usage.

- ✓ ***High agility, scalability and mobility*** – Computing resources are available in real time, on demand, anywhere, on any device and are not limited to the physical constraints of MDAs' owned infrastructure.

- ✓ ***Simplified, connected Whole-of-Government (WoG) approach*** - MDAs are able to share information via interoperable cloud services, supporting inter-agency collaboration and facilitating the development of integrated WoG, shared cloud delivered services.

- ✓ ***Strategic ICT Delivery*** – MDAs' ICT personnel work alongside business managers to deliver strategic objectives and enhance service delivery, while dedicating minimal resources to the management of physical assets.

- ✓ ***Holistic Information Security protocols*** - MDAs are able to leverage the capabilities of mature cloud providers with robust, best practice information security protocols to monitor and respond to threats. Secure, cloud services align with and complement MDAs security policies and practices that are standardised and documented.

- ✓ ***Resilient services that ensure business continuity*** - The failure of one component of cloud delivered services has little impact on overall service availability and reduces the risk of downtime. MDAs adopt cloud services that are consistent with their business continuity and disaster recovery plans.

- ✓ ***Risk-based Decision Making*** - Agencies identify, assess and understand the risks of cloud services, including the security and privacy of data being stored and maintained by third party providers and duly consider these risks in their cloud services planning process.

6. Scope

The Cloud Policy applies to all Government Ministries, Departments and Agencies (MDAs).

7. Objective: Maximising the Value of Cloud Computing

Mindful of the realities of our economic circumstances, the Government's adoption of cloud computing in its various forms will be progressive and adaptive. Initially, when procuring new or existing ICT services, a "consider cloud"[4] policy is prescribed, wherein public sector organisations must fully evaluate the potential of a cloud-based solution among its choice set.

This "consider cloud" policy allows for the incorporation of experience gained over time in the rollout of WoG cloud computing based solutions and platforms. As the associated cloud economics, risks and benefits within Trinidad and Tobago's unique domestic landscape become more fully understood, the associated policy will be re-examined and updated to reflect changes to the ICT environment and developments in the cloud services space.

Accordingly, the Government's movement to Cloud Computing in its various forms will be multi-phased and progressive rather than a singular event.

The key objectives of the Cloud Policy are to:

1. Raise the awareness of the potential benefits associated with the use of cloud computing solutions by Government to deliver more agile, scalable and responsive public services. ***Appendix II*** outlines benefits associated with cloud delivered services.

2. Provide strategic direction and clarity for the wider adoption of appropriate cloud computing services across the public sector, with appropriate consideration for data classification, information security management and structured processes.

[4] An approach that mandates MDAs to consider cloud-based ICT delivered services as part of its ICT strategy

3. Establish the various mechanisms through which cloud computing resources can be securely and responsibly accessed by the public sector.

4. Encourage the use of cloud delivered services and applications where they are secure, fit for purpose and appropriate for the relevant class of data.

5. Develop a holistic understanding of the econometrics of the delivery of national ICT. Subsequent to this, to realise the elimination of wasteful duplication of ICT infrastructure through the use of cloud based, shared services and platforms, where relevant and secure.

6. Enable and support collaborative cloud computing initiatives across the public sector aimed at facilitating best practice exchange and continuous service delivery improvements.

8. Practical Considerations

MDAs need to consider the following factors when procuring cloud services:

- value for money – including that the service is fit for purpose - as defined in The Public Procurement and Disposal of Public Property Act, 2015;
- reducing total cost of operation (TCO) of ICT;
- adequate security - as defined at Section 12.2 of this Policy
- the realisation of timely deployment and implementation timelines

9. Action Plan

An action plan will be developed for the implementation of cloud delivered services by MDAs with requisite timelines and milestone activities.

10. A Hybrid Cloud Computing Model for GoRTT

The Government Communications Backbone, GovNeTT, will be leveraged to deliver a National Government Cloud (GovNeTT NG). A hybrid cloud deployment model in a multi-tenanted environment will be used to deliver all three (3) cloud service models – Software as a Service (SaaS); Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) to MDAs and the wider public sector.

The hybrid Government Cloud (GovNeTT NG) environment provides MDAs with a mixture of on-island private cloud for confidential, restricted or sensitive data that requires a higher set of controls than data stored in the public cloud.

Private cloud services, for the storage of MDAs confidential and restricted data, will be hosted within GoRTT approved Data Center(s).

10.1 Software as a Service (SaaS) via GovNeTT NG

SaaS has tremendous potential to unlock new levels of collaboration across the public sector. SaaS in the form of cloud productivity applications (email, forms, spreadsheets, etc.) will be provisioned to MDAs by GovNeTT NG. Government email is the property of the GoRTT and should be used for work related purposes. All files, documents, spreadsheets and other content created using the cloud productivity tools provided through GovNeTT NG, remain the property of GoRTT. Permission rule tiers will be established.

Confidential data and personally identifiable information (PII) must be used in accordance with applicable data protection and privacy laws when using cloud productivity applications. Data loss prevention (DLP), malware scanning and other security protocols must be employed to ensure compliance.

10.2 Opt-out of GovNeTT NG

MDAs are required to utilise the cloud services available through the Cloud Service Provider Catalog via GovNeTT NG. Where situations exist that preclude the use of accredited CSPs, the organisation must utilise the opt-out clause of this policy. Exceptions for opting-out of GovNeTT NG are:

a) for reasons of national security;

b) where the current sectoral or MDA regulations prohibit the use of GovNeTT NG;

c) where international arrangements provide for access to proprietary cloud delivered services and specialised content, outside the scope of GovNeTT NG such as that which obtains in the area of Health Care.

d) where educational and non-profit arrangements provide for cloud delivered services, software and productivity suites at no cost, or at a cost lower than what obtains via GovNeTT NG.

Such “opt-out” cases must be documented by the relevant Permanent Secretary or Agency Executive and should be submitted to the Permanent Secretary of the Government Agency charged with responsibility for the administration of Government and National ICT Policy. Where necessary, the Ministry of Finance will be engaged with regard to the disapproval of funding for unauthorised, non-GovNeTT NG contracts. ***Appendix III*** provides additional details on the “opt-out” process.

11. Cloud Service Providers Catalog

An online Cloud Service Provider (**CSP**) Catalog will be created to list all accredited domestic and international, public and private cloud service providers whose prices and service offerings can be accessed by MDAs. Annual performance reviews will be conducted on the accredited CSPs and this information will be made available to GoRTT stakeholders.

The benefits of the CSP Catalogue are as follows:

- ✓ **Pricing transparency saves time and reduces duplication of CSP assessments.** Through the use of a pre-accredited CSP list and the publication of pricing, the process will have greater transparency. MDAs will not have to use their internal resources to undertake individual assessments of CSPs.

- ✓ **Ensures CSPs meet Government’s Cloud Standards.** The accredited list of cloud vendors would be pre-vetted to ensure that they are financially stable and that their services meet or exceed the mandatory risk management and security controls for Government Cloud Standards and. For the operations of Government Cloud, all contracts and service level agreements are subject to the Laws and Regulations of the Republic of Trinidad and Tobago. Any claims raised shall be resolved in the legal jurisdiction of the Republic of Trinidad and Tobago.

12. Essential Considerations for the Adoption of Cloud Computing Solutions

The Cloud Policy document outlines the key considerations and conditions for the use of cloud computing in the public sector. It recognises that each MDA will have specific needs for data security, information and security assurance and privacy, which will influence its choice of cloud services and deployment models. Thus, all relevant security and privacy risk impacts must be thoroughly assessed and managed by individual MDAs based on their unique mandate, budget and needs, providing for the adoption of a level of security which is at least equal to the minimum whole-of-government (WOG) Information Security Standard.

12.1 Human Capital Requirements

Cloud adoption requires personnel with the requisite training and experience in cloud technologies, and the possession of different skill sets in order to ensure successful migration to or deployment in the cloud. This includes system architects, data security and privacy experts, data analysts, cloud application designers/developers, and cloud workload administrators. Organisations must therefore be fully aware of the new skills that are required to support operations in the cloud and ensure that such skills can be accessed over the lifetime of the cloud engagement.

12.2 Digital Information Security Management

The Government's intent is to make greater use of cloud computing as a component of improved public service delivery and good governance. It is to be noted that the use of cloud services is closely related to digital service delivery which naturally gives rise to concerns about the security of digital assets. Members of the public sector, business community and citizenry must be confident that their data is securely held and protected from unauthorised access, change or disclosure. As ICTs are increasingly interwoven in the delivery of public services, digital information security becomes even more critical. Thus, GoRTT's digital assets must be appropriately protected when they are in use, at rest or in transit.

Consequently, when considering the adoption of cloud services, greater focus must be placed on the establishment of robust information security management systems in accordance with the standards set out in:

i. ISO/IEC 27000 (Series) - *Information Security Management Systems*

ii. ISO/IEC 27017 – *Guidelines for Information Security Controls applicable to the Provision and Use of Cloud Services* *iii.* ISO/IEC 27018 - *Code of practice for data protection controls for public cloud computing services (includes personal data proctection)*

iv. ISO 22301 - *Societal security – Business Continuity Management Systems: Requirements*

v. ISO 31000 - *Risk Management:- Principles and Guidelines*

vi. ISO/IEC 27018 – - *Code of Practice for Protecting Personal Data in the Cloud*

The Information Security Management System protects the confidentiality and integrity of information data sets by applying a risk management process, which is a precursor to proper data classification.

In support of this Cloud Policy, at a minimum, the following digital information systems security objectives must be achieved by MDAs:

- Confidentiality – assurances to prevent unauthorised access to information.
- Integrity – assurances that information is accurate, valid, and protected against unauthorised alteration or destruction.
- Availability – assurances to provide authorised users with timely and reliable access to information.

It is noteworthy, that with the availability of security services via cloud delivery, encryption capabilities must be used to secure data in the cloud. Additionally, MDAs can access these capabilities through the cloud to protect their sensitive and confidential data.

12.3 Data Classification

It is beyond the scope of this Policy to prescribe a data classification scheme for each MDA and it is expected that a Data Classification Policy for GoRTT will be developed in consultation with the Ministry of Communications, the Ministry of the Attorney General and Legal Affairs and the Ministry of National Security.

It is recognised that as an interim measure, Data Classification must be implemented by all GoRTT MDAs so that they may determine and assign relative values of risk and sensitivity to the data they possess. All data cannot be treated in the same way or assigned the same value.

The process of data classification creates various categories of data based on the applied risk assessment and sensitivity criteria. Such risk assessment must also take into consideration which confidential data cannot be held in the public cloud due to existing legislation or national interest concerns.

The mandates of various MDAs and the type of data which they handle differ greatly across the public sector. Individual MDAs must consider their specific, identified risks when developing a data classification process. A key outcome of the data classification process will be the identification of sensitive confidential data assets and personal identifiable data sets, which will impact the selection of cloud service that can be legally considered.

In the interim, in the absence of a formal Data Classification Policy for GoRTT, Government data must be subjected to a privacy impact assessment and an appropriate classification scheme. The Policy recommends a classification scheme comprising the following four (4) tiers:

Tier 1: Unrestricted Data (UD)

Data intended for internal and/or external use, with minimal controls. Disclosure of data will not impact the reputation of MDA's or of GoRTT. Examples include annual reports, stakeholder related data, media releases, data that may have marketing benefits, data available on public facing websites and data accessible through the Freedom of Information Act, 1999 (FOIA).

Recommended Implementation Mode: Accredited cloud service providers

Tier 2: Official or Sensitive Data (OSD)

Information created in the course of carrying out the day-to-day activities of MDAs and intended only for authorised distribution within individual MDAs. Examples include internal policies, company newsletters, training information, general work related data about the MDA, marketing plans, clients and staff working papers.

Recommended Implementation Mode: Accredited public cloud providers with Multi-level Access Control must employ encryption technology.

Tier 3: Confidential, Sensitive Personal Information (CSPI)

Data that is subject to specific access authorisation and controlled distribution, whether recipients are internal or external. All recipients must require such data in order to perform their duties effectively. Unauthorised disclosure of this data will cause severe damage to the confidentiality of MDA's operations and/or lead to financial penalties. Some examples of CSPI are management accounts, system configurations, helpdesk data, private or commercially important data and confidential internal communications.

Recommended Implementation Mode: Accredited private cloud services exclusively for Government use must employ encryption technology.

Tier 4: Strictly Confidential, Secret

Data of the highest confidentiality whose unauthorised disclosure will have a significant, material impact on the major interests, business operations of the MDA and the wider GoRTT. Assignment of the Strictly Confidential classification must be authorised by a relevant senior authority on a case-by-case basis. This tier will include Cabinet Minutes, legal documents, employee personal files, payroll data, procurement and contract data and national security data.

Recommended Implementation Mode: Accredited private cloud services exclusively for Government use must employ encryption technology.

Guidelines for protecting the integrity of the data, the systems and their users are provided at ***Appendix IV***.

12.4 Compliance with Legislative Framework

MDAs are required to comply with the current range of legislative frameworks addressing the security, privacy, access, storage, management, retention and disposal of Government data and personally identifiable information.

The primary legislation in this regard are detailed below:

i. ***Exchequer and Audit Act, Chap. 69:01 and Amendments*** - provides for control and management of the finances of Trinidad and Tobago, and more particularly for payments, by and to GoRTT, by means of electronic funds transfer.

ii. ***Financial Intelligence Unit of Trinidad and Tobago Act, Chap. 72:01*** -establishes the Financial Intelligence Unit of Trinidad and Tobago, for the implementation of the anti-money laundering policies of the Financial Action Task Force.

iii. ***Freedom of Information Act, Chap. 22:02*** - provides to members of the public, a general right (with exceptions) of access to official documents of public authorities unless otherwise exempted.

iv. ***Data Protection Act, Chap. 22:04*** - provides for the protection of personal information in the custody of an organisation, whether public or private. It must be noted that the Data Protection Act governs the conditions under which personal information can be stored or processed outside of the jurisdiction of Trinidad and Tobago.

v. ***Electronic Transactions Act, Chap. 22:05*** - gives legal effect to electronic documents, electronic records, electronic signatures and electronic transactions.

vi. ***Interception of Communications Act, 2011*** - provides the legal framework within which public or private communications, which are being transmitted by means of a public or private telecommunications network, can be lawfully intercepted.

vii. ***Computer Misuse Act, Chap. 11.17 -*** prohibits any unauthorised access, use or interference with a computer and for other related matters. It is to be noted that this Act is under active review and may be replaced by the Cybercrime Bill after due consideration by the Legislative Review Committee.

12.5 Legislative and Regulatory Review

It is acknowledged that there may be antiquated regulations that govern various aspects of the operations and auditing of the Public Service which are not conducive to the technological realities of cloud computing.

Such laws and regulations will need to be reviewed and updated on a case- by-case basis, once identified by an MDA as being a constraint on the adoption and use of cloud services to fulfill a business need or obtain requested service delivery enhancements.

12.6 Data Ownership

GoRTT MDAs retain full control and ownership of their data at all times. Service contracts and other Service Level Agreements (SLA) related to provisioning of cloud services for Government agencies shall clearly state that any data migrated to the cloud remains the property of the contracting Government entity, regardless of who owns, manages or operates the cloud service. The Government contracting entity retains rights of data access, retrieval, migration, modification and deletion of data exported into cloud services.

Identification of the actual geographic locations where data storage and processing will occur is required. The Republic of Trinidad and Tobago will be the jurisdiction which governs the operation of the contract, and application of privacy, confidentiality, access and information management. GoRTT MDAs will also retain the Intellectual Property Rights (IPR) for any specific development that it pays for or elaborates internally.

12.7 Funding, Asset Management and Enterprise Licensing Impact

Traditional national ICT investments by GoRTT have been predominantly capital intensive involving the acquisition and maintenance of hardware assets. These assets have a tangible value with accompanying depreciation. Funding for such capital expenditure investments typically falls under the regime of the Public Sector Investment Programme (PSIP). In contrast, cloud delivered services are provided as a service to be funded out of recurrent expenditure votes. When doing their annual budget exercise, MDAs need to be cognisant of the shift from capital budgets to operating budgets.

Where GoRTT has enterprise software licences agreements comparative cost benefit analysis will be undertaken to evaluate what benefits can be realised through SaaS.

12.8 Procurement Compliance

All activities to evaluate, acquire and manage cloud delivered services will be done in compliance with the guidelines of the Public Procurement and Disposal of Public Property Act of 2015.

Cloud computing must be assessed on the same basis as other alternative ICT solutions when considering investments and expenditure to:

- upgrade existing legacy computing systems;
- acquire new ICT systems or operations;
- upgrade or replace hardware and software; and
- explore new technology options when existing operating agreements expire.

Total cost of ownership (TCO) assessments must be done. TCO assessments consider the acquisition cost, ongoing warranty, maintenance, sparing and disposal costs through the life cycle of the computing solutions under consideration. It is the responsibility of each MDA to undertake the necessary information security and data risk assessments and regulatory review to ensure compliance within their unique environment.

While cloud delivered services may offer several advantages, they may not always be the best solution. Critical factors such as national security considerations or other existing policy directives must also be weighed, as needed.

12.9 Contract Agreements

The Ministry with responsibility for ICT, in collaboration with the Office of Procurement Regulation, will develop a suite of standard documents, terms and conditions for contracting cloud delivered services for MDAs. These contract terms are critical in ensuring MDAs retain control and ownership of their data in compliance with existing regulations and legislation.

12.10 Interoperability and Portability

In order to avoid CSP lock-in, GoRTT MDAs will ensure that service level agreements (SLAs) and service contracts include necessary provisions for data and application portability such that data movement on and off various cloud platforms can take place as required. MDAs must evaluate exit costs as part of their assessment process before utilising a cloud service. Interoperability of all Cloud Service workloads are to be based on GoRTT's:

- e-Government Interoperability Framework (e-GIF), which defines a variety of tactical and interoperability standards that simplify the integration of Information Technology systems within the public sector; and

- e-Government Omnibus Technical Standards (e-GOTS) which complements the e-GIF and defines technical standards to support application and service interoperability.

13. Practical Methodology for Migration to Cloud

It is acknowledged that business process re-engineering and new skill sets will be required at the operational ICT Division's level to effect cloud migration programmes. In order to provide greater clarity and a migration process framework for practitioners, the following migration methodology is provided:

STEP 1. Situational analysis

- Take stock of your current environment and available budget. Non-sensitive workloads that involve the use of information in the public domain may be prioritised for migration first.

- Identify how ICT resources are aligned to objectives and how costs are optimised. These include Government websites, public archives, application development and testing environments.

- Take stock of the status of the technology life cycle of your current ICT portfolio of hardware, software and operating systems.

- Identify potential benefits from cloud migration that are specific to your organisation. For example, faster time to deploy, ease of management given current staff availability and on-hand skill sets.

- Conduct an assessment of the technical resources required to ensure successful cloud adoption and determine availability of such resources. Develop a plan to bridge any gap that exists.

- Conduct risk assessment of the data classification sets under consideration for migration. Get information from your Legal Division on the existing regulatory and legal frameworks that require compliance. Based on your data classification and risk impact assessment, identify the suitable cloud environment and platform that can be considered.
  Software should be used on a trial basis, before purchase, to ensure that the organisation's needs can and will be met.

- Identify alternative technology solutions and associated costs of cloud environment and platform. Weigh the merits of replacing existing applications with new ones or complete architecture redesign.

- Submit your requirements, desired outcomes and risk assessments to your Procurement Department or Officer, who will then undertake the necessary cost benefit analysis and procurement activity.

If the cloud delivered service is the selected solution to be procured, proceed to Step 2

STEP 2. Provision

- Create a cloud migration roadmap, with defined timelines, responsibilities and reporting lines.

- Establish a project management team for the cloud migration project.

- Track migration progress of the plan in an iterative manner and identify any potential risks.

STEP 3. Manage and Monitor

Post migration, adequate testing of the cloud environment needs to be performed before existing solutions are decommissioned. Testing should be performed on the basis of both normal usage scenarios and extreme load scenarios.

Monitor performance and service delivery against contracted terms and key performance objectives.

Contractual provisions to be monitored:

- Mechanisms and procedures that prevent data loss such as CSP responsibilities for backup, failover or redundancy, should be documented;

- Provisions for testing of continued accessibility, usability, integrity of data post-migration;

- Provisions for restoration of services and disaster recovery;

- Provisions for the return of data and/or transfer of data to new CSP (where possible) when exit is required due to the termination of the agreement with the incumbent CSP;

- Provision for notification and remedies for CSP regarding breaches and outages;

- Agreed performance reporting and audit schedules.

14. Best Practice Exchange

The Ministry with responsibility for ICT will establish best practice exchanges. Outcomes realised by various MDAs in their cloud adoption journey will be documented and shared. This facilitates continuous improvement in evaluating technology options across the public sector based on a growing repository of case studies. This approach enables agencies to learn from each other and fosters collaboration.

15. Policy Review

This policy will be reviewed at least once every twelve months from the date of approval and circulation. This will facilitate the incorporation of post-implementation feedback and/or required updates. Monitoring and evaluation efforts will be focused on quantifying the savings due to the use of cloud delivered services and qualitative assessments of public service delivery improvements.

APPENDIX I

Cloud Computing: Characteristics and Models

Cloud computing delivers scalable, convenient, on-demand network access to shared computing resources (e.g. networks, servers, storage, applications, and services) that can be quickly provisioned remotely and used with minimal management or service provider interaction. Essentially, cloud computing allows users to easily access remotely supported pooled computing capability without having to procure, build, manage or upgrade these resources.

Cloud computing services are generally standardised and configured by the cloud service provider to maximise economies of scale and minimise implementation timelines.

GoRTT has adopted the widely referenced definitions of the models and characteristics of cloud computing that were developed by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.[5] These are detailed in Table 1: Cloud Computing Overview

Table 1: Cloud Computing Overview

Five Key Characteristics	Three Delivery Models	Four Deployment Models
On-demand	Software as a Service (SaaS)	Private cloud,
Broad Network Access	Platform as a Service (PaaS)	Public cloud
Resource Pooling	Infrastructure as a Service (IaaS)	Community cloud
Measured Services		Hybrid cloud (a mix of cloud deployment models)
Rapid Elasticity		

[5] https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

NIST defines the following characteristics and models of cloud computing:

- ***On demand self-service -*** A consumer can unilaterally and automatically provide computing capabilities such as server time and network storage, as needed, without requiring human interaction with each service provider.

- ***Broad network access -*** Capabilities are available over the network and accessed through standard mechanisms that promote usage by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

- ***Resource pooling -*** The provider's computing resources are pooled to serve multiple consumers, dynamically assigning physical and virtual resources according to consumer demand.

- ***Rapid elasticity -*** Capacity can be elastically provisioned and released according to demand. They appear to be unlimited and can be appropriated in any quantity at any time.

- ***Measured service -*** Resource usage is monitored, controlled and reported, providing transparency for both the customer and the service provider.

Cloud Computing Service Models

There are three (3) cloud service models available.

Software as a Service (SaaS): Defined as software that is owned, delivered and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on usage metrics. Users access these applications through their web browser or another client interface. Users do not have to install, update and maintain software locally. Examples of SaaS are cloud productivity suites which provide email, presentation, spreadsheets and online customer relationship management (CRM) applications.

***Platform as a Service* (PaaS):** A category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. PaaS can be delivered in two ways; as a public cloud service from a provider where the consumer controls software deployment with minimal configuration options with the provider providing the networks, servers, storage, OS, 'middleware' (e.g. Java runtime, .NET runtime, integration), database and other services to host the consumer's application; or as a private service (software or appliance) inside the firewall, or as software deployed on a public infrastructure as a service.

***Infrastructure as a Service* (IaaS):** The provision of a virtualised environment of servers, data storage, computer processing and software that can be shared by several users. The service provider is responsible for the maintenance of the physical infrastructure.

Cloud Computing Deployment Models

Cloud services can be provided through one or more of these four (4) deployment models:

Public cloud which is provisioned for open use, wherein the service provider owns and manages the infrastructure, which can be accessed via the Internet. Due to the tremendous capacity of scaling, the highest levels of economies of scale may be realised through public cloud. However, the public cloud also carries security risks associated with its wide availability and ability to shift data geographically. Such potential price efficiencies must be balanced against the risk with due consideration given to the class of data being evaluated.

P*rivate cloud* is provisioned for exclusive use by a single organisation or group of organisations. The pooled computing environment from which the cloud service is provided is dedicated to that specific organisation or customer group. The volume of economies of scale that can be realised is constrained by the size of the aggregate computing networks. Private clouds may exist on or off premise; and may be operated by in-house staff of the organisation or group or by a contracted third party.

Community Cloud is private cloud infrastructure that is provisioned for exclusive use by a specific community of users or organisations. These organisations usually have shared mandates, missions or security requirements. The community cloud infrastructure may be owned and operated by one or more of the organisations in the community or a third party.

Hybrid Cloud is provisioned through a combination of cloud infrastructure of two or more cloud models (private, community or public). The hybrid cloud architecture allows the benefits of the public cloud to be realised while simultaneously providing for the following data in use, in transit or at rest:- application portability, load balancing with greater security, and load balancing with greater control levels.

	Public Cloud	**Private Cloud**	***Community Cloud* / Dedicated Servers**	**Hybrid Cloud**
Description	Multi-tenant environment with pay-as-you-grow scalability	Scalability plus the enhanced security and control of a single-tenant environment	For predictable workloads that require enhanced security and control	Connect the public cloud to your private cloud or dedicated servers — even in your own data center
	Services delivered via Datacentres in developed countries. Well-known Public Cloud Service Providers include: • Amazon Services • Google • Microsoft	Available in T&T from the in-country Cloud Service Providers: • Digicel • TSTT • Fujitsu • CW-Flow • etc.	Fully Managed Dedicated Server Hosting Available in T&T from the in-country Cloud Service Providers	Mix of on premise Cloud Service Providers.
Physical hardware	Shared	Dedicated	Dedicated	Shared + Dedicated
Best for	Non-sensitive, public-facing operations and unpredictable traffic	Sensitive, business-critical operations	Sensitive, business-critical operations, plus demanding performance, security and compliance requirements	Combine public, private and/or dedicated servers, for the best of each
Enhanced security and control	x	✓	✓	✓
Scalable	✓	✓	x	✓
Low cost, utility billing	✓	x	x	✓
Predictable cost	x	✓	✓	✓
Flexible	✓	x	x	✓
Customizable	x	✓	✓	✓
High Performance	x	✓	✓	✓

APPENDIX II
Benefits of Cloud Computing for GoRTT

GoRTT is keen to realise the cost reductions and cost efficiencies which are the main benefits commonly associated with the adoption of cloud computing. It must be stressed that cloud computing can be used as a powerful enabler of better public sector service delivery for citizen-centric programmes. Such improved performance outcomes, can only be realised by concerted and collaborative efforts to re-engineer business processes and pursue prompt implementation by leveraging cloud technologies.

Greater cost efficiencies – Given the small size of the economy, it is critical that the benefits of cost savings and efficiencies from aggregated demand are sought rather than siloed approaches. There are several common ICT requirements and processes across the public sector which facilitate the leveraging of cloud computing within the context of a shared services model.

Scalability – Cloud services can be contracted as required and in the amount required thereby avoiding the acquisition of infrastructure and licences while allowing MDAs to enhance adaptability based on their specific needs.

Continuity of Operations for Government Business and Robust Business Recovery – The public sector is becoming increasingly dependent on ICTs to carry out its day-to-day operations. Cloud computing can support the deployment of more robust and resilient disaster recovery options in the event of a natural disaster such as hurricanes, earthquakes or other disruptive events. Off-island data storage also provides for geographic redundancy in the event of a national catastrophe, natural or manmade.

Faster Deployment of Public Service Enhancements and Innovation – The traditional procurement methodology for national ICT investments can be capital intensive, long and protracted. Reducing the amounts of upfront capital investment and shortening the mobilisation time for ICT projects can lead to faster deployment of enhanced public service programmes and new services. The ability to implement programs faster and adjust workload capacity is particularly valuable for those MDAs that have significant seasonal and time-based demand for their public services such as filing of tax returns or receipt of grants.

It is envisaged that as IT resources are freed from the tasks of asset management and maintenance, innovation can be fostered as their talents are applied towards the creation of innovative custom-built Government applications and data analytics.

Greater command of the economics of national ICT Budgets – The utility-based usage model associated with the cloud service model contributes to greater cost clarity and accountability. This, in turn, supports improved budget control. The return on investments in national ICT can also be captured with greater ease.

Table 2 contrasts the benefits of cloud computing for GoRTT with that of the current environment

Table 2: Benefits of Cloud Computing for GoRTT

Cloud Benefits	Current State
Greater Cost Efficiencies	Fragmented demand and duplicative systems
Improved asset utilisation through aggregated demand.	Government pays for idle, under utilised computing capacity
Government pays for usage of computing resource	Predominantly on premise server and storage installations
Agility and faster deployment of public service enhancements and Innovation	Mobilisation of new service can take between several weeks to several months.
IT resources involved in more strategic activities such as custom application development, information security management and data analytics	IT resources involved in operational activities and asset management and maintenance. Ongoing maintenance cost of legacy infrastructure
Focus on shared services	Focus on asset management.
More robust Disaster Recovery and Business Continuity options	Inconsistent rollout of business continuity programmes
Greater command of the economics of national ICT budget	Lack of clarity on the econometrics of national ICT
Operating Expenditure Model focuses on paying for only what is needed contributing to greater agility and cost-efficiency	Capital expenditure model requires significant upfront investment in often under utilised equipment resulting in wasted capacity and reduced agility and cost efficiency as costs increase over time.

APPENDIX III

Process For Administration of Opt-Out from Whole-of-Government (WoG) Cloud Computing Arrangements

MDAs must seek approval from the Ministry with responsibility for ICT, in conjunction with the Ministry of Finance, to opt-out from agreed cloud delivered services arrangements.

The opt-out process requires that:

- an MDA prepares a short justification based on its genuine business needs, irrespective of the manner in which the alternative cloud delivered service arrangement is funded;
- opt-out requests be submitted by the Permanent Secretary or designated Officer.

Arrangements subject to Opt-Out

The Ministry with responsibility for ICT will consider submissions to set up arrangements which provide clear superior outcomes for the Government and/or the taxpayer over autonomous approaches by MDAs. Generally, these arrangements will possess one or more of the following criteria:

- economy of scale of benefits which do not have a significant adverse impact on wider Government policies;
- enhanced ability to move towards more joined-up services for citizens and businesses;
- improved management and development of scarce ICT skills within the Public Service
- improved operation of the GoRTT ICT marketplace;
- reinforcement of other key priorities of GoRTT such as enhanced service delivery and economic competitiveness;
- reduction and avoidance of duplication of costs;
- enhanced capacity and ability to respond to external ICT related issues and trends; and
- improvement in the management and leveraging of GoRTT's information assets with due regard to privacy concerns as appropriate.

Criteria for Considering Opt-Out Requests

One or more of the following criteria should apply to a request to opt-out of a GoRTT approved CLOUD COMPUTING CONSIDERATION POLICY:-

- The CLOUD COMPUTING CONSIDERATION POLICY cannot be implemented within existing regulations and legislation;
- The application of the policy would create a tangible threat to national security;
- The ability to respond to external ICT related issues and trends will not be improved;
- The ability to manage and leverage the Government's information assets, having due regard to privacy concerns where appropriate, will be enhanced;
- Compliance costs and regulatory burden on citizens and business are reduced. Alternative lower costs to the existing Government Cloud arrangements or no cost cloud delivered services, which are secure and compliant with domestic regulations and legislation, can be realised. These cloud computing resources may be accessed from international and non-profit agencies with which GoRTT has entered into some form of technical cooperation agreements.

At least forty (40) days prior to consideration of a non-Government Cloud arrangement, an opt-out applicant must provide the Ministry with responsibility for ICT with its written justification. Such justification must outline:-

- the activity or activities for which opt-out is required;
- the grounds upon which opt-out is being requested;
- the duration for which opt-out is being sought;
- a short financial analysis outlining the cost of compliance and non-compliance to the MDA and to the whole-of-government;
- an analysis of any significant risks of both the opt-in and the opt-out option; and
- an analysis of the impacts on citizens/clients, both positive and negative, of opting out.

APPENDIX IV
Guidelines for Protecting the Integrity of Data, Systems & Their Users

The following guidelines are to assist in the protection of the system and users while guaranteeing availability, confidentiality and integrity of the data, solutions and related processes:-

- Identify the digital assets (data and information systems) included in the solution and classify them according to their level of criticality to provide the solution with adequate IT security.

- Verify that within the digital assets the following three properties of the data or the information systems are guaranteed:
    - *Availability* : The data and related resources must be available to be accessed by authorised users

    - *Integrity:* Data must be kept complete and unaltered, unless it is modified by an authorised user

    - *Confidentiality:* Avoid data access by UNAUTHORISED users.

- Define who is (are) the party (ties) responsible for the data or for the information systems of the solution.

- Provide adequate processing for the solution based on its level of criticality at the moment of defining the infrastructure that will support it.

- Ensure that the system or platform complies with the following principles to provide a safe and protected environment:
    - Identify all access points to the system or platform, taking into consideration all users and applications that access it, whether local or remote. Keep a registry of every access to the system.

    - Protect the solution by authorising each access to it through authorisation levels linked to each user authenticated on the platform. This will help protect the system against unauthorised access, preventing involuntary or intentional errors.

- Protect and safeguard the system’s security and notify the TTCSIRT of any security events.

- Respond proactively to the detection of a security event, initiating the actions necessary to mitigate and/ or resolve the threat before it causes harm to data and/ or the systems.

- Always have recovery plan that meets the service expectations of users.