وزارة الاتصـــــــالات وتكنولوجيـــــــا المعلومـــــــات
Ministry of Communications and Information Technology
State of Qatar • دولـــة قطـــر

Cloud First Policy

Date: April 2024 | Version: 1.0.0 | Ref: P005

DISCLAIMER / LEGAL RIGHTS

The Ministry of Communications and Information Technology (MCIT) has designed and created this publication, entitled Cloud First Policy with reference P005 (hereinafter referred to as the "Work"), primarily as a resource for government bodies, senior management, IT management, risk management and IT, and IT security professionals in the State of Qatar.

The "Work" has been prepared in accordance with the laws of the State of Qatar and does not confer, and may not be used, to support any right on behalf of any person or entity against the State of Qatar or its agencies or officials. If a conflict arises between this document and the laws of Qatar, the latter shall take precedence. Every effort has been made to ensure the "Work" is accurate, but no warranty, guarantee or undertaking is given regarding the accuracy, completeness or currency of the "Work". Links to other websites are inserted for convenience only and do not constitute endorsement of material at those sites, or any associated organization, product or service.

Any reproduction of this "Work", either in part or full and irrespective of the means of reproduction, shall acknowledge MCIT as the source and owner of the "Work". Any reproduction concerning the "Work" with intent of commercialization shall seek a written authorization from MCIT. MCIT shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent. The authorization from MCIT shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

State of Qatar
Qatar Digital Government
Ministry of Communications and Information Technology
Digital Government Policies and Standards Department

http://www.mcit.gov.qa

e-mail: policy@mcit.gov.qa

Legal Mandate

Article 17[1] of Amiri Decree No. 57 of 2021 sets the mandate and function for the Ministry of Communications and Information Technology (hereinafter referred to as "MCIT") to supervise, regulate, and develop the sector of Information and Communications Technology (hereinafter referred to as "ICT") in the State of Qatar in a manner consistent and aligned with, but not limited to the following:

- Supervising and developing the ICT sector in line with national development needs.
- Supervising the creation of an appropriate regulatory environment for fair competition.
- Supporting, developing, and stimulating the ICT sector and encouraging investment.
- Securing, developing, and raising the efficiency of information and technological infrastructure.
- Raising awareness on the importance of using ICT to advance society, build a knowledge-based digital economy, and improve the life of the individual.
- Implementing and supervising e-Government[2] and Smart Society programs.
- Strengthening government infrastructure and capabilities in the field of ICT.

Furthermore, this policy has additional legal support from the following:

- Amiri Decision No. 47 of 2022 established the Digital Government Policies and Standards Department and its responsibilities which include but are not limited to developing policies, guidelines, and technical frameworks for digital government affairs; proposing draft related legislative tools; setting standards and technical specifications related to digital government; measuring government agencies' compliance with policies, guidelines, and technical frameworks related to digital government affairs.

Strategic Alignment

Qatar National Vision (2030)	Economic Development	Build world-class infrastructure with efficient and effective delivery mechanisms for public services and institutions.
Qatar 2nd National Development Strategy (2018-2022)	Developing a Modern Public Sector	Leveraging technology to build a modern public sector that provides accessible, secure, and robust services across the nation.
Cloud Policy Framework (2022)	Cloud First Policy Recommendation	Unlock efficiency and productivity and create an opportunity for government agencies to provide better services.

[1] Links to all external resources can be found in the Related Legislation and Documents section.

[2] Technical terms and their meaning can be found in the Glossary of Terms and Definitions section.

Document Summary

Name	Cloud First Policy
Version	1.0.0
Document Reference	P005
Document Type	Policy
Summary	This policy requires government agencies working on projects involving new IT systems or technology refreshes to firstly consider and evaluate cloud solutions from cloud service providers who have government-wide agreements (hereinafter referred to as endorsed CSPs[3]). This policy aims to gradually migrate traditional IT infrastructure, platforms, and software to the cloud and take advantage of the benefits of cloud computing which include, but are not limited to, dramatic cost savings, improved security and compliance, flexible and elastic resource utilization, improved agility and delivery speed, simpler data management and integration, collaboration and innovation opportunities, and a reduced carbon footprint. The Cloud Computing and Networks Department within the MCIT supports cloud adoption across government agencies and provides centralized governance which includes the management of cloud credits.
Publishing Date	April 2024
Applicable to	This policy is applicable to all government agencies in Qatar.
Adoption Period	Immediate effect - Government agencies shall prepare a cloud adoption report[4] within 3 months of this policy's publication date.
Owner	Ministry of Communications and Information Technology (MCIT)
Contributor(s)	Cloud Computing & Networks Department, Communications Regulatory Authority, Government Infrastructure Operation Department

** For any feedback or inquiries, please contact policy@mcit.gov.qa*
*** The Cloud Computing & Networks Department can be contacted at sharedservices@mcit.gov.qa*

[3] Refer to Glossary of Terms and Definitions section.

[4] Refer to Appendix 5 for an example report.

Acronyms

AI	Artificial Intelligence
COTS	Commercial Off The Shelf
CSP	Cloud Service Provider
CRA	Communications Regulatory Authority
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IoT	Internet of Things
ITU	International Telecommunications Union
ML	Machine Learning
MCIT	Ministry of Communications and Information Technology
NCSA	National Cyber Security Agency
NIA	National Information Assurance
PaaS	Platform as a Service
SaaS	Software as a Service
SLA	Service Level Agreement

Table of Contents

1 Introduction

Cloud computing has become a highly mature and stable technology driving organizations in nearly every industry sector across the world. It is fundamentally different to traditional on-premise IT and provides access to powerful processing, practically unlimited storage, and a dynamic cost model charging only for resources used.

Adopting the cloud computing paradigm is a necessary prerequisite for Qatar to transition to a fully digitalized nation, achieve its goal of becoming a digital hub for the region, and for government to leverage and adopt disruptive technologies (e.g., AI, ML, Big Data, IoT, etc..). Cloud capabilities in government have been proven to drive savings, improve security, reduce technology duplication and fragmentation, lift productivity and agility, and quickly deliver quality services that meet citizen demands.

Cloud computing is defined as a:

*"paradigm for enabling **network access** to a **scalable** and **elastic** pool of **shareable physical** or **virtual resources** with **self-service** provisioning and administration on-demand" (ITU)*

Cloud computing has the following five distinct characteristics:

On-demand self-service	Broad network access	Resource pooling	Rapid elasticity	Measured service
• Computing capabilities (e.g. server time, network storage) provisioned automatically without requiring human interaction with the CSP.	• Capabilities available over the network. • Accessed through standard mechanisms and thin or thick client platforms (e.g., mobiles, tablets, laptops & PCs).	• Computing resources are pooled together. • Dynamically assigned and reassigned resources* as required by demand.	• Capabilities elastically provisioned and released. • Resources* are automatically controlled and optimized to scale rapidly in line with demand.	• Usage of resources* is monitored, controlled and reported. • Transparency for CSP and the government agency.

** Resources include servers, operating systems, networks, software, application, storage equipment.*

Figure 1: Essential Characteristics of Cloud Computing

This policy requires government agencies to fully evaluate and adopt cloud solutions before any other options. The policy aims to migrate government on-premise IT infrastructure and solutions to endorsed CSPs, and be an example for private entities[5] showcasing the benefits of cloud computing[6] to encourage wider adoption across Qatar.

[5] Private entities can refer to Cloud Computing: A Handbook for SMEs

[6] Refer to Appendix 1 for cloud computing benefits.

The following guidelines, regulatory documents, and any other applicable policies and legislation should be read in conjunction with this document:

- Cloud Policy Framework
- National Information Assurance Policy
- NCSA Cloud Security Policy[7]
- Personal Data Privacy Protection Law
- Data Privacy Guidelines for Regulated Entities

1.1 Background

National strategic engagements have been made with a number of global hyperscalers that have passed Qatar's data residency, security and operational requirements. These endorsed CSPs collectively provide a wide range of cloud services that can be leveraged by government agencies.

The Cloud Computing and Networks Department (incorporated under the MCIT)[8] provides centralized governance and management of cloud credits for use with endorsed CSPs:

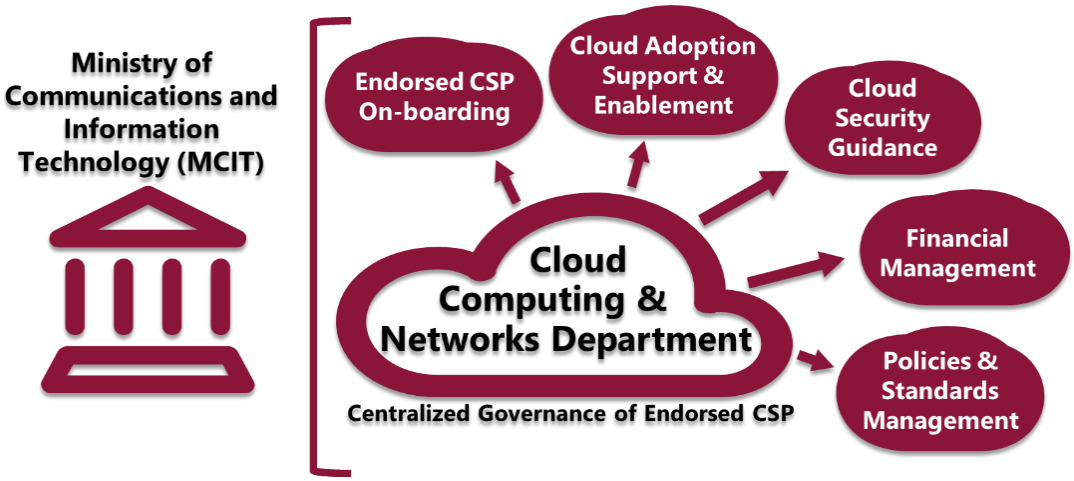

Figure 2: Cloud Computing and Networks Department Support

Furthermore, generic cloud deployment, service, and migration models have been contextualized to better fit government IT solutions and infrastructure. These models are described in the following sections.

[7] The NCSA (previously known as Q-CERT) aims to maintain and regulate national cybersecurity and protect the vital interests of Qatar in the face of cyberspace threats (refer to Amiri Resolution No.1 of 2021).

[8] Cloud Computing and Networks Department can be contacted at sharedservices@mcit.gov.qa.

1.1.1 Cloud Deployment Model

Common cloud deployment models consist of public, community, private, and hybrid approaches[9]; these have been tailored to address the unique data, security, and operational needs of government agencies in Qatar:

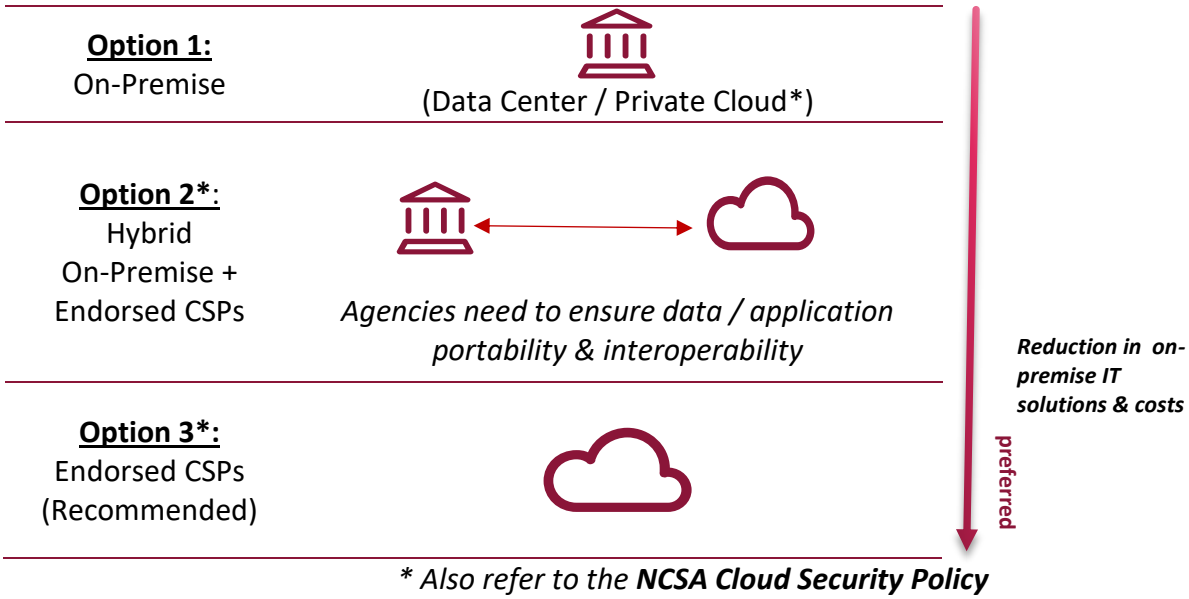

Figure 3: Cloud Deployment Models for Government Services in Qatar

1.1.2 Cloud Service Model

Cloud service models are commonly offered in one of three ways (IaaS, PaaS, SaaS); government agencies should strive to maximize reductions in on-premise IT solution management and costs while meeting data, security, and operational needs.

Management responsibilities are distributed between the CSP and the government agency based on the service model chosen, cloud provider used, and the context of the application. Ultimately the government agency needs to ensure requirements are met, particularly for security (refer to NCSA Cloud Security Policy).

[9] Refer to Appendix 2 for information on generic deployment models.

See below for generic examples of the different responsibilities in each cloud service model (refer to Appendix 3 for further details):

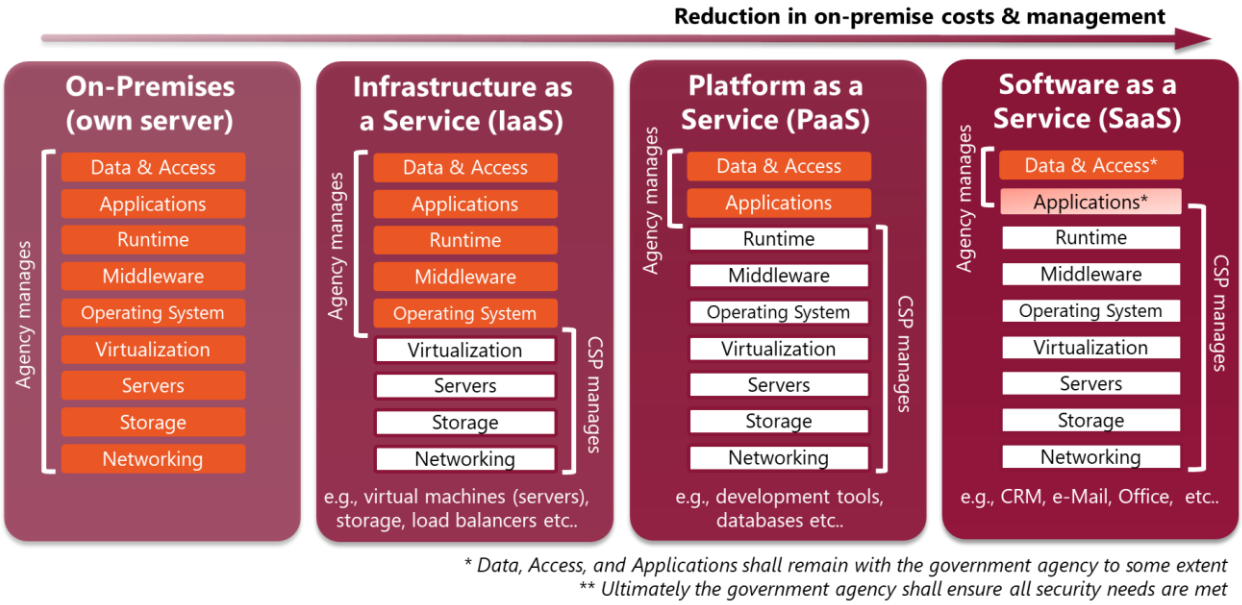

Figure 4: Cloud Computing Service Models

1.1.3 Cloud Migration Strategy

The cloud migration strategy to use depends on the unique context of each government agency (e.g., budget size, resource availability, application architecture, technical ability, business complexity etc.) while considering data, security, and operational needs.

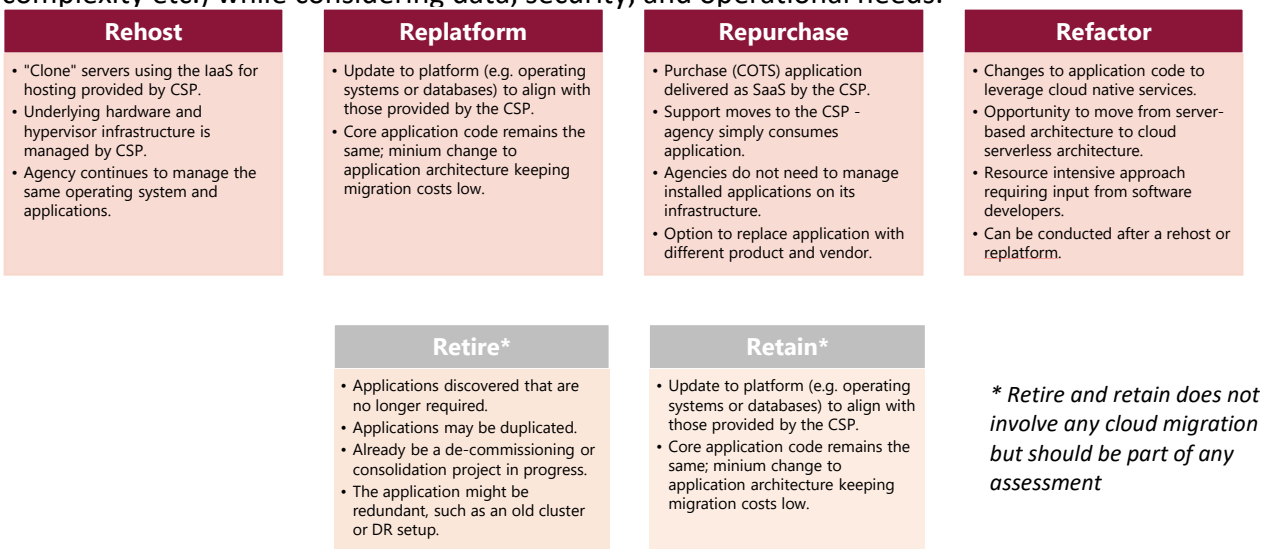

Figure 5: Cloud Migration Strategies (refer to Appendix 4)

2 Policy Objectives

The key objectives of this policy are to:

2.1 Accelerate adoption and migration of government on-premise IT infrastructure and solutions to endorsed CSPs except when deemed unsuitable after full consideration and evaluation (refer to Appendix 4).

2.2 Ensure that government agencies adopt cloud services from endorsed CSPs as the first and primary option when making IT investment decisions to migrating or developing new solutions, or conducting technology refreshes.

2.3 Leverage advantages of endorsed CSPs across government, which include, but are not limited to, cost, scale, resilience, governance, agility, support, optimization, and flexibility (refer to Appendix 1).

2.4 Ensure adherence to applicable policies, regulatory and compliance requirements, laws and legislation, and the use of a data classification approach aligned to the NIA policy, as part of a risk assessment before moving systems and data to the cloud (refer to Appendix 4).

3 Policy Scope and Application

3.1 Applicable to all government agencies that make investments to procure, migrate, or develop IT infrastructure, platforms, applications, and e-Services.

3.2 Applies to any planned and future investments of government systems, platforms, or infrastructure components as well as the maintenance, renewal, or upgrade of existing hardware and software solutions.

3.3 Encompasses all categories of cloud service models, cloud deployment models and cloud migration strategies including, but not limited to, those mentioned in section 1.1.

3.4 Operates subject to legal, security, and privacy considerations, and in compliance with relevant policies, regulations, and laws as mentioned in this document and otherwise applicable in Qatar.

3.5 Provides a general approach to risk assessment (refer to Appendix 4) taking into consideration information and data classification along with other principles identified in, but not limited to, the NIA Policy, the NCSA Cloud Security Policy, and the Personal Data Privacy Protection Law. Government agencies should refer to relevant regulatory and legislative documents applicable in Qatar, which are mentioned, but not limited to, those documents listed in section 1.

3.6 Any technical or investment related assessments in regards to cloud migration and adoption not included in this policy can be conducted by government agencies to meet their individual needs; these may include, but are not limited to areas such as cost (TCO / ROI) and scalability.

4 Policy Provisions

This policy requires all government agencies to apply the following provisions:

4.1 Adoption and Governance

4.1.1 Government agencies shall first consider the suitability of the cloud platform and services offered by endorsed CSPs before evaluating alternatives when planning IT investments; this includes but is not limited to procuring, migrating, or developing IT infrastructure, platforms, applications, and e-Services.

4.1.2 All cloud solutions shall be aligned with the data classification approach in the NIA Policy, the NCSA Cloud Security Policy, applicable Cloud Computing and Networks Department guidelines, standards and policies, and any other relevant laws and regulation.

4.1.3 Cloud services shall not be utilized by government agencies without developing an exit strategy for individual services and the CSP. On enactment of the exit strategy the government agency shall inform the Cloud Computing and Network Department.

4.1.4 Government agencies shall integrate cloud services into business continuity and disaster recovery plans.

4.1.5 Government agencies shall prepare and complete a cloud adoption report (refer to Appendix 5) within 3 months of the publication of this policy.

4.1.6 Exceptions to the use of platforms and services offered by endorsed CSPs shall be documented with a detailed assessment for submission and authorization by the Digital Government Policies and Standards Department in the MCIT (policy@mcit.gov.qa). If deemed necessary, the Cloud Computing and Networking Department shall either directly evaluate or provide subject matter support during the evaluation of any exception requests.

4.2 Data Classification

4.2.1 Each government agency shall define and apply a data classification scheme within their organization aligned with the NIA Policy before migration of information and services to the cloud.

4.2.2 The data classification scheme shall implement at least five levels (C0 public, C1 internal, C2 limited access, C3 restricted, C4 national security/confidential) as outlined in the NIA Policy.

4.2.3 Data classified as C4 is exempt from this policy; government agencies are directed to follow the relevant provisions in the NIA Policy and any other relevant laws and regulation.

4.2.4 Government agencies shall identify all Personally Identifiable Information (PII)[10] for consideration when risk assessing any potential cloud migration and adhere to the Personal Data Privacy Protection Law and Data Privacy Guidelines for Regulated Entities.

4.2.5 Based on a risk assessment exercise, the government agency shall determine whether to migrate government data and apply the applicable safeguard or ultimate safeguard [encryption by default] during and after migration, particularly on the most highly classified government data, leveraging the risk management policies and standards covered in the NIA Policy and NCSA Cloud Security Policy. The assessment shall take into consideration the operational challenges, the security controls available to mitigate potential security and privacy risks, and the risk appetite of the government agency (refer to Appendix 4).

4.3 Data Ownership and Management

4.3.1 Government agencies shall retain data ownership throughout the lifecycle of the data; the CSP shall only act as the custodian of data during the government agency's use of its cloud services.

4.3.2 Government agencies shall ensure the CSP has appropriate data destruction procedures in place which are aligned to the NIA Policy, the NCSA Cloud Security Policy, and any other legal, regulatory, and security requirements.

4.3.3 Government agencies shall where possible use standard data formats to aid interoperability and data portability, and ease the enactment of the exit strategy when disengaging from a CSP or service (refer to section 4.1.3).

4.3.4 Government agencies shall identify and document in the exit strategy, data sets and related meta data that may need to be extracted, transferred, or converted to support the return of data to the government agency. On enactment of the exit strategy the government agency shall inform the Cloud Computing and Network Department.

4.4 Risk Management and Compliance

4.4.1 Government agencies shall regularly or when deemed necessary assess and identify risks associated with the data and services hosted on the CSP. Identified risks shall be included and integrated into the government agency's internal risk management processes.

4.4.2 Government agencies shall include business continuity management, disaster recovery plans, and the cloud exit strategy in their risk assessments.

4.4.3 Government agencies shall identify and implement adequate technical, operational, and security controls on the CSP in compliance with legislation, standards, and policies to mitigate security and privacy risk.

4.4.4 Government agencies shall regularly and when deemed necessary test the viability of the cloud exit strategy based on priorities, business criticality, service impact, and anticipated

[10] Refer to Related Legislation and Documents for links to the Personal Data Privacy Protection Law and Data Privacy Guidelines for Regulated Entities.

risks. The Cloud Computing and Network Department shall be informed when performing these tests.

4.4.5 Government agencies shall regularly or when deemed necessary audit controls the agency has implemented on the CSP which include but are not limited to those implemented for the mitigation of security and privacy risks. Corrective actions shall be taken as necessary to achieve legal and regulatory compliance and confirm the required assurance level is met.

4.5 Implementation Progress and Review

Agency responsibilities:

4.5.1 Government agencies shall within 3 months of publication of this policy prepare and complete a cloud adoption report (refer to Appendix 5).

4.5.2 Government agencies shall integrate cloud services into business continuity and disaster recovery plans.

4.5.3 Government agencies shall develop exit strategies for individual services and the CSPs used. On enactment of the exit strategy government agencies shall inform the Cloud Computing and Network Department.

4.5.4 Government agencies shall be responsible to ensure and demonstrate compliance with relevant policies and laws in Qatar and other applicable international laws and regulations when moving data, services, and other information to the cloud.

4.5.5 Any exceptions to this policy shall be requested from the Digital Government Policies and Standards Department and shall be accompanied by a detailed assessment and supporting justification (refer to 4.1.6).

4.5.6 Government agencies shall provide an up-to-date cloud adoption report (refer to Appendix 5) as and when requested.

Cloud Computing & Networks Department (incorporated under the MCIT) responsibilities:

4.5.7 The Cloud Computing and Networks Department shall on-board government agencies to the endorsed CSPs and provide governance in areas which include, but are not limited to, demand and portfolio management, risk management and compliance, tenant management, budget and financial tracking, policies, guidelines and best practices.

4.5.8 The Cloud Computing and Networks Department shall support government agencies to adopt the use of cloud services in areas such as, but not limited to, cloud architecture and models, contracts and SLAs, and cloud security guidance.

4.5.9 The Cloud Computing and Networks Department shall manage the distribution of cloud credits to all government agencies using appropriate demand forecasting methods. The Cloud Computing and Networks Department shall evaluate, track and monitor consumption of cloud credits by government agencies on an ongoing basis.

4.5.10 The Cloud Computing and Networks Department shall produce a quarterly consumption report, identify areas for cost optimization, and when necessary provide government agencies with recommendations.

4.5.11 The Cloud Computing and Networks Department shall improve in-house cloud capabilities across government by identifying and facilitating the training of government employees.

4.5.12 The Cloud Computing and Networks Department may issue additional or supplementary procedures, guidelines, and best practices from time to time to support this policy.

4.5.13 The Cloud Computing and Networks Department shall when requested by the Digital Government Policies and Standards Department evaluate any requests for an exception to any part of this policy (refer to 4.1.6).

MCIT responsibilities:

4.5.14 MCIT may issue additional or supplementary procedures, guidelines, and best practices from time to time to support this policy.

4.5.15 MCIT shall evaluate exceptions to this policy as requested by government agencies to the Digital Government Policies and Standards Department (policy@mcit.gov.qa). All requests must be accompanied by a detailed assessment which may be shared and jointly evaluated by the Cloud Computing and Networks Department (refer to 4.1.6).

4.5.16 MCIT shall monitor implementation of this policy by government agencies and may at any time request information and/or a detailed report on the adoption of this policy.

5 Glossary of Terms and Definitions

Term	Definition
Agency	Government agency/entity, unless the term is used or referred to in a specifically different context.
Artificial Intelligence	Theory and development of intelligence demonstrated by computer systems to mimic "cognitive" functions that are expected to require human intelligence such as learning, problem solving, speech recognition, decision-making, and language translation.
Big Data	Extremely large data that is too complex to be dealt with by traditional data-processing methods and requires new computational methods to help reveal complex patterns, trends, and associations, especially relating to human behavior and interactions.
Cloud Computing	Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand where examples of resources include servers, operating systems, networks, software, applications, and storage equipment (ITU).
Cloud Credits	Cloud credits are tokens which can be used to access and use services on the endorsed CSPs.
Cloud Security Policy	Refers to the National Cyber Security Agency Cloud Security Policy for government agencies.
Cloud Service	Service offered, according to a contract, over the internet to subscribers or customers, including to individuals or enterprises, whether for free or for a fee, that provides on-demand access to a shared pool of computing resources and that allows subscribers or customers to access, store, transmit, or process data and information.
Cloud Service Provider	A third-party company offering a cloud-based platform, infrastructure, application, or storage service (e.g., SaaS, IaaS, PaaS).
Community Cloud	Shared cloud computing environment targeted to limited set of organizations which generally share similar security, privacy, performance, and compliance requirements.
Disruptive Technology	New technology that completely changes the way things are done. It displaces a well-established product or technology, changing the way businesses, consumers, or industry functions.

Term	Definition
e-Government	Use of ICT to more effectively and efficiently deliver government services to citizens and businesses. This involves application of ICT in government operations, achieving public ends by digital means, while improving the internal workings of government agencies. It broadly aims to produce sustainable solutions through a reduction in financial costs and transaction times by integrating workflows, processes, and effectively utilizing resources across agencies.
Endorsed CSP	Cloud service provider who has signed a government-wide agreement and met the regulatory and legal requirements of Qatar in areas such as, but not limited to, data residency, security, access, privacy.
Government agency / entity	All ministries and public institutions under ministries or Council of Ministers in Qatar, unless the context of usage clearly indicates a different meaning.
Hybrid Cloud	When the cloud infrastructure is a composition of two or more distinct cloud deployment model (private, community, or public) but are bound together by standardized or proprietary technology that enables data and application portability.
Infrastructure as a Service (IaaS)	Infrastructure as a service model of cloud wherein organizations avail infrastructure services over cloud from the cloud service provider.
Internet of Things (IoT)	System of interrelated, internet-connected objects that are able to collect and transfer data over a wireless network without human intervention.
International Telecommunication Union (ITU)	Agency of the United Nations for information and communications technology issues. It aims to enable the growth and sustained development of telecommunications and information networks, and to facilitate universal access so that people everywhere can participate in, and benefit from, the emerging information society and global economy.
Machine Learning	Use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data.
On-premise	Software that is installed and runs on computers or servers that physically reside on the premises of the organization using the software, rather than on a remote facility.
Platform as a Service (PaaS)	Platform as a service model of cloud wherein organizations avail platform services over cloud from the cloud service provider.

Term	Definition
Private Cloud	Cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Public Cloud	Cloud infrastructure provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Smart Society	Harnesses the potential of digital technology, data-based decisions, connected devices, and the use of digital networks to empower society, improve people's lives, strengthen the economy, and improve the effectiveness of institutions.
Software as s Service (SaaS)	Software as a service model of cloud wherein organizations avail software application services over cloud from the cloud service provider.
Tenant	Single cloud consumer consisting of a group of users, generally belonging to a single organization, using cloud services and supporting infrastructure. Single tenancy provides a single instance of a service and supporting infrastructure without any sharing, while multi tenancy shares the service and supporting infrastructure with other consumers.

6 Related Legislation and Documents

The following table provides links to all relevant documents and papers referenced in this policy. Every effort is made to ensure these links are valid, but there may be times when resources may not be available due to being deleted, moved, or replaced.

Legislation	Article 17 of the Amiri Decision Number (57) for the Year 2021 Amiri Decision No. 47 for the Year 2022 Amiri Resolution No. 1 for the Year 2021 Law No. 13 for the Year 2016 - Personal Data Privacy Protection
Policies, Standards, or Frameworks	Cloud Computing A Handbook for SMEs CRA Cloud Policy Framework Data Privacy Guidelines for Regulated Entities National Information Assurance Policy (NIA Policy) NCSA Cloud Security Policy (previously known as Q-CERT)
Other Links	ITU - Cloud Computing – Overview Qatar National Development Strategy (2018-2022) Qatar National Vision (2030)

APPENDICES

Appendix 1: Cloud Computing Benefits and Categories

The adoption of cloud computing solutions offered by endorsed CSPs can provide, but is not limited to, achieving the following benefits:

1. Reduce total cost of ownership and CAPEX (Capital Expenditure), by improving IT utilization, aggregating demand, and removing duplication in government IT spending.
2. Improve cyber security resilience by using internationally accredited platforms, with best-in-class cyber security standards leveraged by the endorsed CSPs.
3. Elevate the quality of government online services and shared services, through agility in addressing evolving business demands and improving end-user experience.
4. Provide computing capabilities unilaterally (e.g. server time, network storage) as needed automatically without requiring human interaction.
5. Access data, systems, and platforms over the network and through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
6. Achieve rapid elasticity, through provisioning and releasing of services, in some cases automatically, to scale rapidly outward and inward commensurate with demand. This is especially beneficial for government agencies which deals with hard to predict business requirements.
7. Control and optimize resource utilization automatically (e.g., storage, processing, and bandwidth) by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., the number of active user accounts).
8. Adopt advanced and disruptive technologies, due to the fact that some technologies may require scarce IT talent to provision and maintain, which can be provided by Cloud, allowing government agencies to experiment and adopt advanced technologies easily and for relatively low investments.
9. Reduce carbon emission footprint, through reduction of energy consumption, waste, and carbon emissions, as a result of eliminating multiple on-premise data centers.

Appendix 2: Cloud Deployment Model

A cloud deployment model is a specific configuration of environment parameters such as the accessibility and proprietorship of the deployment infrastructure and storage. Deployment types can vary depending on who controls the infrastructure and where it is located.

Typical deployment models include the following:

- **Public Cloud:** All hardware, software, and other supporting infrastructure (e.g., servers and storage) is owned, operated, and managed by the CSP. You share hardware, storage, and network devices with other organizations or cloud "tenants". You access services and manage your account using a web browser. Public cloud deployments are frequently used by private users as well as government agencies, financial institutions, and mid-large size organizations. Microsoft Azure, AWS and GCP are examples of a public cloud.
- **Private Cloud:** Consists of computing resources used exclusively by one business or organization. Can be physically located at your organization's on-site datacenter or hosted by a third-party service provider. In a private cloud, services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organization. Private clouds are often used by government agencies, financial institutions, any other mid- to large-size organizations with business-critical operations seeking enhanced control over their environment to customize resources and meet specific IT requirements.
- **Community Cloud:** Resembles a private cloud except there are several organizations with similar backgrounds that share the infrastructure, related resources, and costs. These organizations have uniform security, privacy and performance requirements and use a multi-tenant architecture which can help these companies enhance their efficiency, as in the case of joint projects.
- **Hybrid Cloud:** Combines on-premise infrastructure, or private clouds, with public clouds so organizations can reap the advantages of both. Data and applications can move between private and public clouds for greater flexibility and more deployment options. For instance, the public cloud can be used for high-volume, large-scale computing needs such as intensive compute jobs and the private cloud (or other on-premise infrastructure) used for managing archival storage of long-term corporate records.

Appendix 3: Cloud Service Model

Cloud computing is generally offered as three different service models – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

- **Infrastructure-as-a-Service (IaaS):**
  - Provides processing, storage, networks, and other fundamental computing resources where the agency is able to deploy and run arbitrary software, which can include operating systems and applications.
  - The agency does not manage or control the underlying cloud infrastructure, but does have control over operating systems, storage, deployed applications, and possibly limited control of selected networking components.
- **Platform-as-a-Service (PaaS):**
  - The agency is able to deploy onto the cloud infrastructure created or acquired applications using programming languages, libraries, services, and tools supported by the cloud service provider.
  - The agency has control over the deployed applications and possibly application-hosting environment configurations, but management or control of the underlying cloud infrastructure including network, servers, operating systems, or storage is done by the cloud service provider.
- **Software-as-a-Service (SaaS):**
  - The cloud service provider's applications running on a cloud infrastructure can be used by an agency. Applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email), or a program interface.
  - The agency does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Appendix 4: Assessment of IT Investment

The diagram below provides a step-by-step approach that government agencies may use to risk assess and plan new IT investments[11]. The Cloud Computing and Networks Department can provide support during planning and adoption:

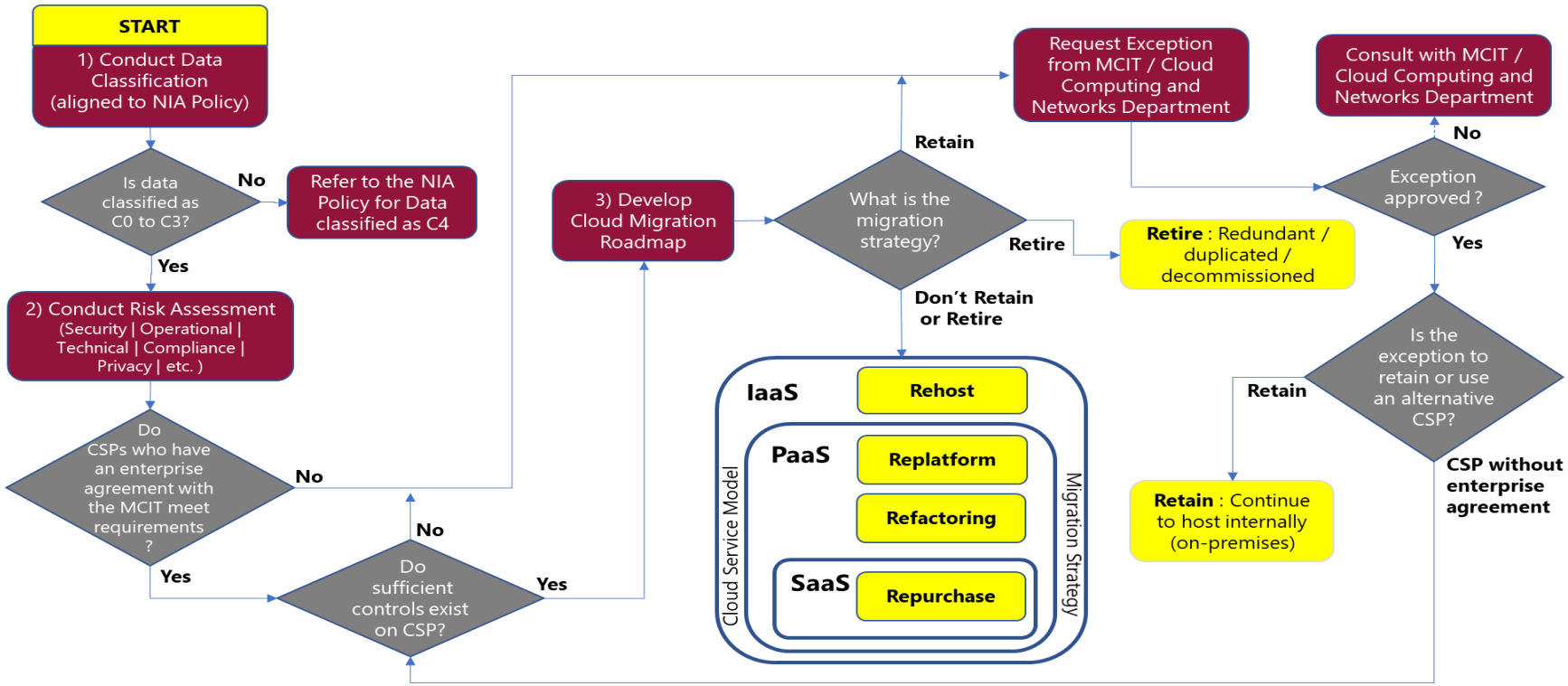

Figure 6: Indicative Approach for IT Investment Assessment

[11] Any other technical or investment related assessments not included can be conducted by government agencies to meet their individual needs (refer to section 3.6).

Appendix 5: Cloud Adoption Report

The following table provides an example of the information that needs to be included in the report. Each row depicts an individual solution and / or a planned IT investment within the government agency. Government agencies can use this information to create a roadmap and include more or less detail as required, such as other dependencies, drivers, priorities, or costs.

Software / Application / Tool Name	Data Classification	Security / Operational Risk Assessment	Identified Controls	Application Dependency	Cloud Suitability	Envisaged Benefits	Migration Strategy	Cloud Service Model	Planned Migration Date (if known)	Comments (Challenges / Cloud Computing & Networks Depart Requests)
Ticket Management Tool	C2	Passed	Implement encryption in transit	None	Yes	Cost Reduction, business agility, high availability	Replatform	PaaS	Q1 2023	
. . . . .										

Document Control

Version	Date	Amendments	Author
1.0.0	01/04/2024	Release of policy	MCIT

Prepared by
Digital Government Policies & Standards Department
Ministry of Communications &
Information Technology
Version 1.0.0 2024

E-Mail: policy@mcit.gov.qa
www.mcit.gov.qa