INFORMATION &
eGOVERNMENT AUTHORITY

Cloud First Policy

General Directorate of Governance and Operations

Version 1.0 | 14 JUNE 2017

Table of Contents

Definitions/Glossary

Acronyms / Abbreviations	Definition
iGA	Information and eGovernment Authority
ICT	Information and Communication Technology
SCICT	Supreme Council for Information and Communication Technology
ICTGC	Information and Communication Technology Governance Committee
CSP	Cloud Service Provider
SLA	Service Level Agreement

Policy statement

The Bahraini Government is committed to modernizing government information and communication technologies (ICTs) and will lead by example in using cloud computing services to reduce costs, increase security, increase productivity, and develop excellent citizen services,

The Kingdom of Bahrain will adopt a Cloud-First approach with the aim of:

- Reducing the cost of government ICT by eliminating duplication of solutions and fragmentation in the technology environment, and leveraging the efficiencies of on-demand provisioning of ICT services;
- Increasing security by using accredited platforms;
- Increasing productivity and agility, and thus improving citizen services.

In order to achieve this, all government agencies of the Kingdom of Bahrain will evaluate cloud-based services when undertaking all ICT procurements. The decision on the appropriate ICT delivery model will be based on an assessment of each application, incorporating fitment of purpose, cost benefit analysis and achieving value for money over the life of the investment. This assessment is best achieved by using any of the well-established tools available in the market, either from the identified cloud service provider and/or a non-attached third party.

This document sets out general guiding principles for a “cloud first” approach for government ministries and agencies to consider in adopting cloud computing solutions as a primary part of their information technology planning and procurement.

Entities Affected by this Policy

This policy is applicable to all government entities who are looking to host their data, applications or services in the centralized cloud environment, in accordance with the overall government direction to use a cloud-first approach to support cost optimization in ICT.

It is also applicable to iGA, as they would be the interface between the cloud service provider and government entities, and ICTGC, who will govern the overall implementation of this policy.

Who Should Read this Policy

ICT leadership of all Ministries and Government Entities.

Policy Principles

This policy is based on the following driving principles:

- ICT at entity level must focus on functional excellence and delivering higher business value
- ICT Infrastructure is one key candidate for national level consolidation and optimization
- Standardized infrastructure management enables
    - optimization of infrastructure cost
    - Improvement in service quality
    - improved security
    - efficient business continuity
- Promote holistic “cloud first “approach while respecting the Kingdom of Bahrain and every ministries roles, legislation, and mandates.
  The following rationale of this principle applies to:
    - To reduce redundancy and associated complexity across the ministries and agencies

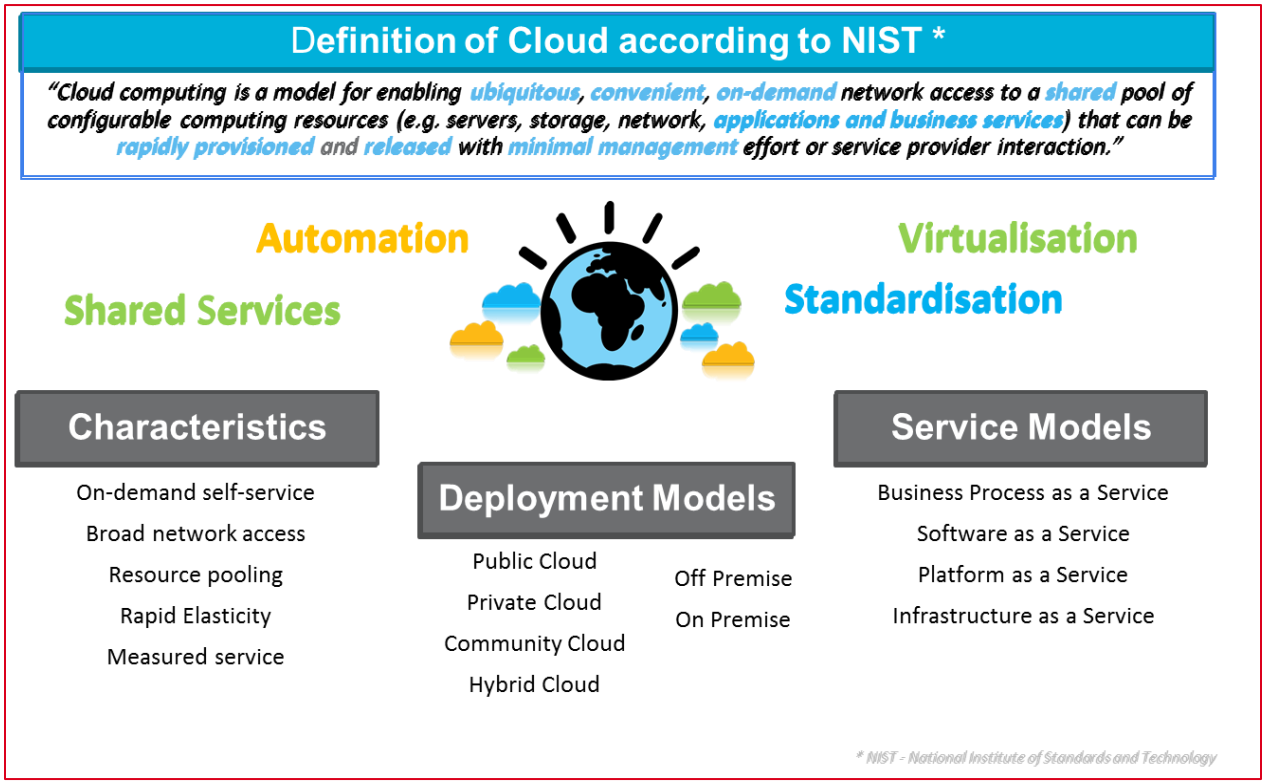
- To design IT infrastructure with a "one government" approach, to facilitate changes in government business processes in an easier and quicker way
- Enable cost optimization and risk reduction across government through leveraging common platform and information systems for cross-government service delivery

Overview of Cloud Computing

There are many different definitions for cloud computing. The Kingdom of Bahrain government has adopted the **National Institute of Standards and Technology** (NIST) definition that defines cloud computing as:

"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

This section provides a brief overview of the essential characteristics of cloud computing together with the cloud service and deployment models. It is recommended that agencies familiarize themselves with the NIST definitions to ensure that they are able to identify and understand the risks associated with different cloud service and deployment models.



Essential Characteristics

The following provides an overview of the five essential characteristics for cloud computing as defined by NIST[1]:

[1] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- **On-Demand Self-Service –** customers are able to provision resources (e.g. a virtual server or email account) without any interaction with the service provider's.
- **Broad Network Access –** customers are able to access resources over networks such as the Internet using a ubiquitous client (e.g. a web browser) from a range of client devices (e.g. smartphones, tablets, laptops).
- **Resource Pooling –** the service provider's computing resources are pooled to serve multiple customers. Typically, virtualization technologies are used to facilitate multi-tenancy and enable computing resources to be dynamically assigned and reallocated based on customer demand.
- **Rapid Elasticity –** resources can be quickly provisioned and released, sometimes automatically, based on demand. Customers can easily increase or decrease their use of a cloud service to meet their current needs.
- **Measured Service –** customers pay only for the resources they actually use within the service. Typically the service provider will supply customers with a dashboard so that they can track their usage.

Deployment Models:

- **Public cloud -** The cloud infrastructure is 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.
- **Private cloud -** The cloud infrastructure is 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.
- **Community cloud -** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Hybrid cloud -** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).

Service Models:

- **Business Process as a Service (BPaaS) -** The capability provided to the consumer is any type of horizontal or vertical business process that's delivered based on the cloud services model. These cloud services — which include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) — are therefore dependent on related services.
- **Software as a Service (SaaS) -** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer 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.

- **Platform as a Service (PaaS) -** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **Infrastructure as a Service (IaaS) -** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Detailed Purpose of Policy

This policy provides guidance to all government entities in the Kingdom of Bahrain, as the Kingdom moves towards a common operating environment for all government entities, leading to:

- **Reduction in cost for both hardware and platforms.** Outsourcing government services to cloud computing results in immediate reductions of large capital outlays for infrastructure and maintenance costs. Up to date, best of class solutions also become immediately available to government agencies through cloud provisioning.
- **Improved manageability and productivity of ICT solutions.** Government ICT resiliency and security is improved and made consistent with upgrades to both hardware and software being managed by the service provider.
- **Better integration between services.** More effective collaboration is enabled as agencies are more easily able to share resources across institutions, improving efficiency, and enabling creativity in delivering public services.
- **Operational continuity and business recovery.** With centralized and redundant data storage and backups, business recovery and data retrieval during times of crisis becomes faster and more cost effective.
- **Greater budget control.** A ‘pay for what you use’ model means that government agencies can purchase as much or as little resource as needed, and only when needed. Cloud scalability results in systems usage being dialed up or down as it is required. Transparency of the utility-based pricing structure means that spending caps and alerts can be implemented to further assist in budget control.
- **Greater agility.** Cloud computing streamlines development, support and hosting of ICT solutions, resulting in improved service performance and faster deployment of services. It reduces the amounts of ICT infrastructure required to be built and owned by government agencies, shifting the focus from management of infrastructure to delivery of services.

Operational Framework

In order to achieve these benefits, the following aspects must be incorporated in the overall process for ICT solution development and delivery.

Application/Service Migration Criteria

Government entities are required to use cloud services for new ICT services and when replacing any existing ICT services, except if:

- it can be shown that an alternative ICT deployment strategy meets special requirements of a government agency and
- it can be shown that an alternative ICT deployment strategy is more cost effective from a Total Cost of Ownership (TCO) perspective, and demonstrates at least the same level of security assurance than a cloud computing deployment.

In using cloud services to reduce costs, improve productivity and develop efficient services, Government entities are to ensure that the cloud service selected is *(refer to Cloud Assessment documents)*:

- fit for purpose,
- provides adequate management of risk to information and ICT assets as defined by the relevant security principles, and
- adheres to local legal and regulatory requirements.

In using cloud services to reduce costs, improve productivity and develop efficient services, Government entities are to:

- consider new major hardware / software projects as a trigger for evaluating and adopting cloud services;
- adopt cloud based services for testing and development needs;
- consider potential of using cloud services for hosting public facing websites;
- evaluate private, community, public or hybrid cloud services for operational systems as defined by ICTGC guidelines.

Cloud Security Principles

The benefit of migrating government workloads and data onto commercial cloud is the ability to enhance overall data security. Cloud service providers engaged by government agencies will be required to meet international security standards, and ensure appropriate certification. They will abide by all relevant industry standards, for example, international security standards such as ISO 27001, Service Organization Controls Report (SOC) 1 and 2; and will adhere to any additional certifications required by specific industries, such as the Payment Card Industry Data Security Standard (PCI DSS), and Cloud Security Alliance (CSA) certification and audit, as well as others.

Government agencies should collaborate with the entity responsible for Information Security in Bahrain to establish a security framework which applies a risk management approach towards its own data control requirements (see Data Classification), and align this with international standards and certifications, as well as industry standards. The precise level of security requirements for contracted cloud services should be determined by the contracting agency based on an assessment of data risk. Stipulated security controls can include any one or more of the following:

- Physical and environmental security
- Business continuity management and incidence response
- Inventory and configuration management
- Data encryption

- Access controls, monitoring and logging
- Network security and monitoring.

Security Framework

Managing the security of contracted cloud services is a responsibility that is shared between the entity responsible for Information Security in Bahrain, contracting agency and the cloud service provider, with the entity responsible for information security defining security controls *in the cloud*, contracting agency align to it, while the cloud service provider is responsible for the security *of the cloud*. In short the data itself remains under the ownership and control of the data owner at all times. The level of responsibility on both parties depends on the cloud deployment model type, and agencies should be clear as to their responsibilities in each model.

Data security depends upon:

1. Meeting security requirements for each data classification level; and
2. Employing standardized tools and procedures for audit.

All data that can be migrated to the commercial cloud will need to meet the necessary security requirements for accreditation, and be verified by international cloud security standards. Commercial cloud service providers should provide logical security audit on data access, including logs and audit trails to ensure the prescribed security and privacy requirements are met.

Government agencies must collaborate with the entity responsible for Information Security in Bahrain to perform the logical audits and continuous security monitoring to ensure cloud services meet the agreed-upon data confidentiality and integrity, that there have been no data breaches, and that data and workloads are continuously available.

Data Classification

An important component of any comprehensive security policy is a policy for classifying data, allowing government agencies to appropriately protect different types of data, while discouraging wasting resources on unnecessary and costly security controls for less sensitive information. Most government organizations handle comparatively little *highly* sensitive information (*refer to Government Data Classification Guidelines and State Secrete Law*).

Nonetheless, with a data classification framework and an understanding of the required security controls in place, government agencies can then decide on assuring that appropriate controls have been designed and implemented relative to the level of security classification, and to ensure that they are operating effectively on an ongoing basis.

Mitigation and Back-Up

Agencies need to have in place mitigation and redundancy contingencies. It is the responsibility of each government agency to ensure that they have a mitigation and back-up plan for their data and services. These plans need to ensure at a minimum:

- Having service continuity in times of disaster or emergency
- No government data loss occurs without recovery.

A mitigation and back-up plan should include backing-up data in a second location in two regions so as to ensure (i) full data protection, (ii) continued and uninterrupted service, and (iii) data recovery.

Data Sovereignty

The benefits of cloud are best realized when there are no data residency restrictions placed on data. Such restrictions undermine the economies of scale and security benefits to be gained from shared computing infrastructure. Access to data in the cloud is dependent on security controls, and agencies concerned with extraterritorial access to data owned by the government should select cloud vendors with the appropriate security standards and controls.

Open Data

Globally, governments are increasingly making their non-restricted data available for the public to discover, access, and use. These open data initiatives facilitate the development of public services, fuel entrepreneurship, accelerate research and scientific discovery, and create efficiencies across multiple sectors. Government entities should endorse the open data principle and, where technically feasible and economically reasonable, make non-restricted data available to other government agencies and the public through the cloud. In keeping with this principle and policy, government agencies should likewise manage their data assets to promote openness and use for the public good.

Roles and Responsibilities

This policy is **approved by SCICT**, developed and reviewed by ICTGC, and implemented by Government entities and iGA. Any changes or deviations from this policy will need a review by ICTGC, and approval by SCICT.

The implementation of the policy will be monitored and governed by ICTGC and SCICT.

In addition, the following roles and responsibilities for each stakeholder, involved with the policy implementation, have been listed below.

Government Entity

- The Heads of the Government entities are responsible for ensuring all aspects of this policy and guidelines are applied within their entity.
- All Government employees involved in procuring cloud based services, applications or platform hosting services for the Government entity must adhere to this policy (refer to *ICT Procurement Practice*).
- The business owner is responsible for the application functionality and support.
- The business owner will ensure optimal sizing and detailed analysis of usage, incorporating seasonal spikes in workloads, to enable accurate budgeting for the cloud services required.
- Monitoring and ensuring the performance of the applications is as per the stated SLA.
- The entity shall monitor usage of the cloud services and provide a monthly usage report to ICTGC. This is to ensure that the usage does not exceed the budgeted limit for the entity.

iGA

- Act as the interface between cloud service provider and government entities.
- Ensure relevant SLAs are defined for the applications based on the entity requirements.
- Monitor and govern SLAs agreed with cloud service provider.
- Provide support and guidance to entities in assessment and identification of applications to move to the cloud.
- Provide technical support to modify applications and get them cloud ready.

ICTGC

- ICTGC will maintain an oversight on the implementation of this policy.
- ICTGC will audit the government entities for compliance at its discretion, at regular intervals as well as on an ad hoc basis.
- Shall act as the arbitrator in cases if dispute between the various government entities

SCICT

- SCICT set the strategic direction for Cloud initiative and oversight the Cloud Strategy implementation.

References Document

IGA Related Policies

- Web Hosting Security Policy
- Password Security Policy
- GDN Connectivity Policy
- Wireless Security Policy
- Bespoke Development vs COTS Policy
- Deployment and Hosting Policy

Related Procedures

- Cloud Applicability Assessment
- Cloud Deployment Checklist and Procedure

Related References

- Government Data Classifications
- State Secret Law
- Service Catalog and Service Classification
- Cloud Adoption Roadmap and Capability Development Plan
- ICT Procurement Code of Practice