KSA Cloud First Policy

Ministry of Communications and Information Technology

October 2020

رقمي
DIGITAL SAUDI

وزارة الاتصالات
وتقنية المعلومات
MINISTRY OF COMMUNICATIONS
AND INFORMATION TECHNOLOGY

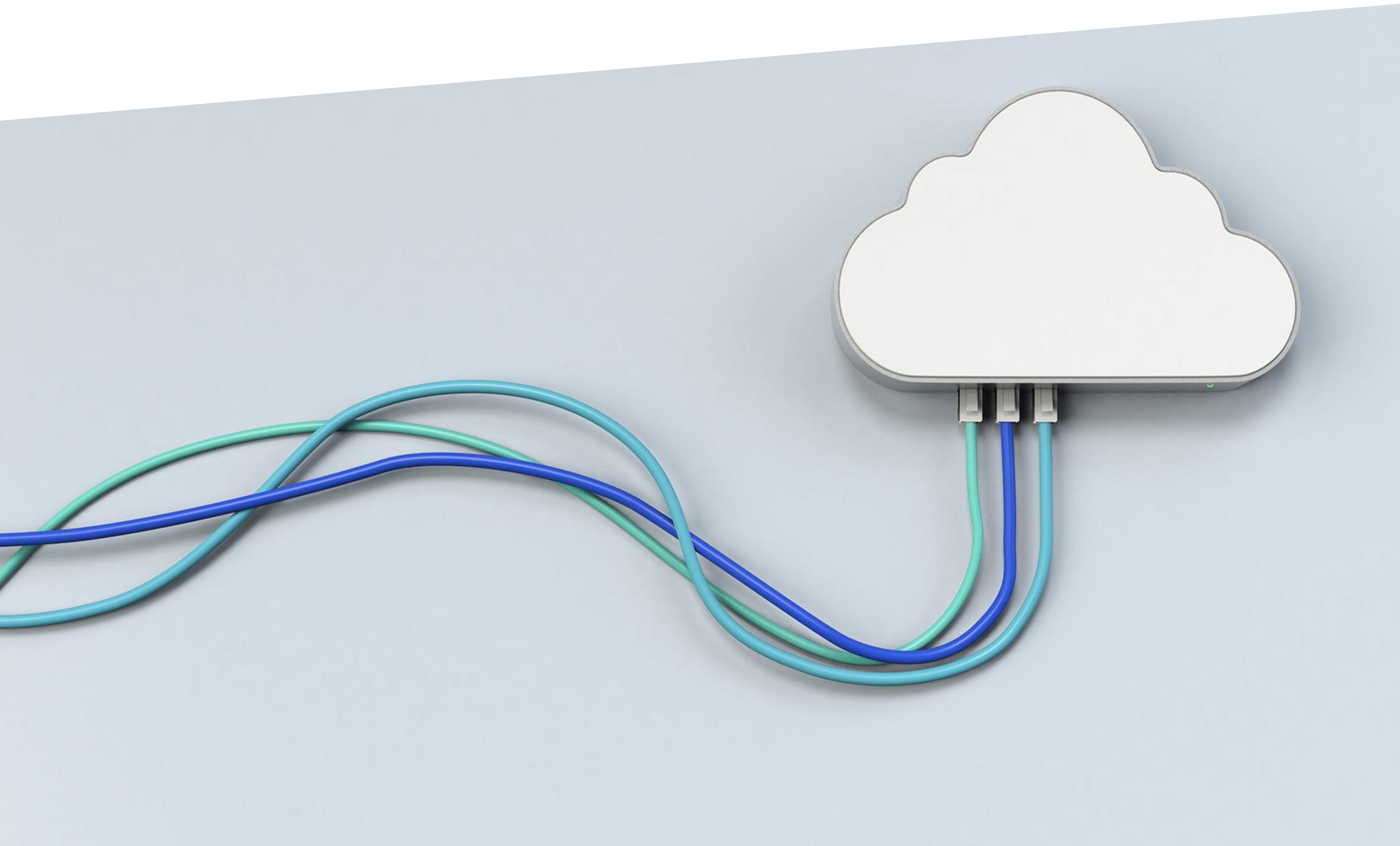


Table of Contents

Executive summary

- For any new IT investment, civilian government entities should consider Cloud solutions as opposed to internal / traditional solutions
- Civilian Government entities are not allowed to buy or build new data center infrastructure, unless stated otherwise in this policy for some specific cases. Only Government owned Cloud Service Providers (CSPs) such as NIC are allowed to build data centers.
- When adopting cloud services, except for data classified as 'secure' and 'top secure' that must be hosted in Government Cloud Service Providers, government entities should first consider approved Commercial Government Cloud Service Providers. In the case of the requirements being not met, Government Cloud Service Providers can be relied upon.
- The Cloud computing adoption team at Yesser will drive the Cloud adoption, check technical and commercial requirements and the National Data management Office will supervise the implementation of the data classification in the government entities in line with set guidelines. The cybersecurity requirements by The National Cybersecurity Authority (NCA) will be enforced on CSPs that want to serve government entities.
- Government entities must always prioritize Cloud solutions in the following sequence: first Software as a Service (SaaS), then Platform as a Service (PaaS), and lastly Infrastructure as a Service (IaaS).

Purpose of this document

This document details KSA's" Cloud First Policy" which is a policy that covers Governmental entities (as specified in the "Scope of the policy" section). The goal is to accelerate the adoption of Cloud computing services by directing these entities to consider Cloud options when making new IT investment decisions. The private sector is encouraged to follow the same exercise by having an internal CFP.

This policy was defined in line with the key pillars of KSA's ambitious Vision 2030. The policy hence caters for the National Information Center's (NIC) strategy – the entity that will serve as the primary Cloud Service Provider (CSP) for Government related data.

The Kingdom of Saudi Arabia is one of the leading countries in the ICT sector in the Middle East and North Africa (MENA) region and is well positioned to capitalize on this Cloud computing opportunity, through becoming one of the best integrated infrastructure services and technically advanced in the Cloud computing industry and the ICT industry in general.

This document complements the Cloud computing regulations issued or to be issued by other governmental entities.

Overview of Cloud Computing

Cloud computing[1] is a model which enables 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. Cloud models are composed of five Essential Characteristics, three Service Models and four Deployment Models.

Key characteristics of Cloud computing

Cloud computing leverages several elements including scale, virtualization, resilience, cost efficiency, service orientation, agility, etc. These elements are combined under the NIST definition into five key characteristics:

1. ***On-demand self-service:*** Unilateral provisioning of computing capabilities, such as server time and network storage, provisioned by the end-user, without requiring human interaction with each service provider.
2. ***Broad network access:*** Availability of capabilities over the network with accessibility through standard mechanisms that promotes usage by the consumer through different platforms (e.g. phones, laptops and PCs).
3. ***Resource pooling:*** Pooled computing resources to serve multiple consumers using a multi-tenant model, with different physical and virtual resources assigned and re-assigned based on demand. There is a degree of location independence, the customer may be able to specify location at a higher level of abstraction (e.g. country, state, or datacenter) but not the exact location of the provided resources. Examples of resources include storage, processing, memory, network bandwidth and virtual machines
4. ***Rapid elasticity:*** Rapid and elastic provision of capabilities to quickly scale resources up and down – this is done in some cases automatically. To the consumer, capabilities available for provisioning are often (almost) unlimited and can be purchased in any quantity at any time
5. ***Measured service:*** Automatic controlled and optimized resources are used by leveraging a metering capability at some level of abstraction, appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service

Service Models

Cloud computing, in its core, offers three different service models, which provide applications, platforms and infrastructure as a service. These service models (illustrated in Figure 1) provide some to all the IT support necessary to deploy an IT solution.

[1] As per the definition of National Institute of Standards and Technology (NIST). MCIT is aware of the standards ISO/IEC 17788:2014 and ISO/IEC 17789:2014 and believes NIST's Cloud Computing standard is more suitable to this policy at this stage.

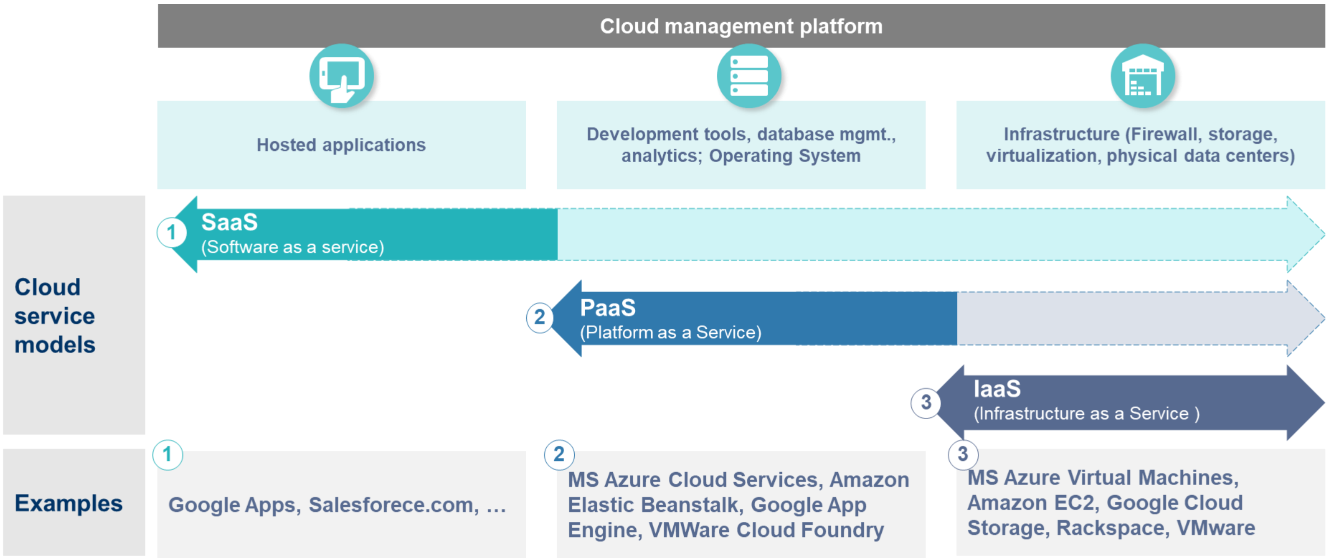

Cloud management platform
Hosted applications
Development tools, database mgmt., analytics; Operating System
Infrastructure (Firewall, storage, virtualization, physical data centers)
Cloud service models
1
SaaS
(Software as a service)
2
PaaS
(Platform as a Service)
3
IaaS
(Infrastructure as a Service)
Examples
1
Google Apps, Salesforece.com, …
2
MS Azure Cloud Services, Amazon Elastic Beanstalk, Google App Engine, VMWare Cloud Foundry
3
MS Azure Virtual Machines, Amazon EC2, Google Cloud Storage, Rackspace, VMware

Figure 1 – Cloud computing service models

Software as a Service (SaaS): The capability provided to the consumer is to use the Cloud Service Provider's (CSP's) applications running on a cloud platform and infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g. web-based email). The consumer does not manage or control the underlying cloud platform and infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Examples may include, but are not limited to:

- Government applications
- Internet services
- Virtual desktops
- Enterprise Resource Planning (ERP) systems
- Customer Relationship Management (CRM) systems
- Communication software (email, instant messaging)

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure of the CSP consumer-created or acquired applications, these applications are created using programming languages and tools supported by the CSP. 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 application hosting environment configurations. Examples may include, but are not limited to:

- Application development
- Database and database management (DBMS)
- Middleware (Web MQ, WebSphere, etc.)
- Testing and developer tools
- Directory Services

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources. It's up to the consumer to decide what software is deployed and operated, 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, deployed applications, and possibly limited control on select networking components (e.g. firewalls). Examples may include, but are not limited to:

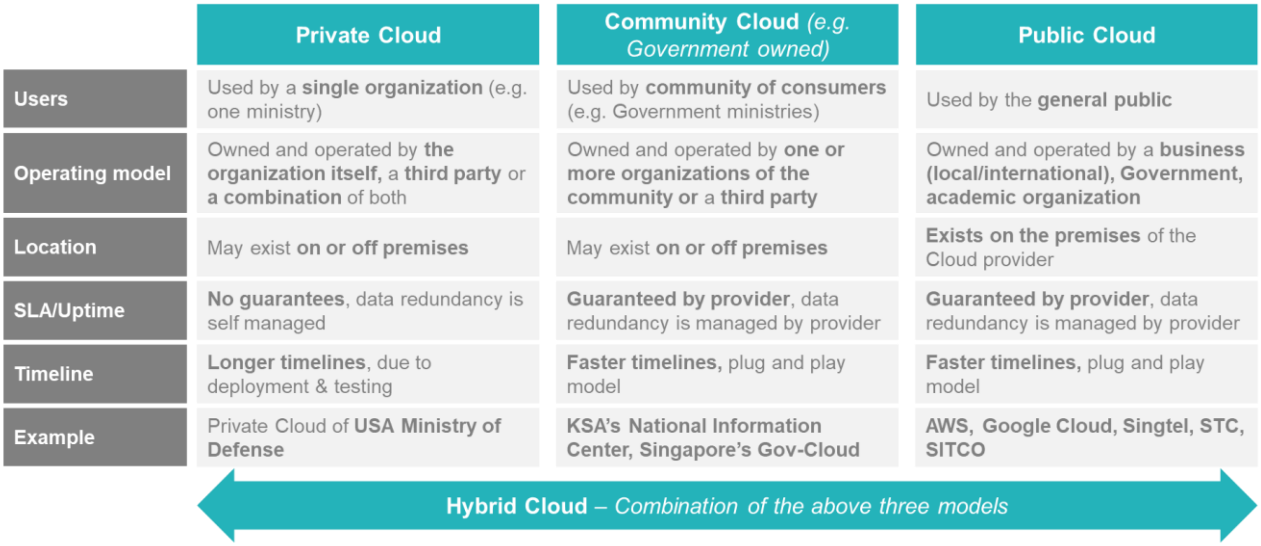
- Mainframes
- Mid-tier Servers
- Storage
- IT Facilities/Hosting Services
- Virtual Machines

Depending on the selected service model, users of the Cloud services will outsource certain portions of the IT value chain to the CSP. Figure 1 provides an overview of the scope covered by each of the service models. For instance, in the Software as a Service (SaaS) model, the CSP will provide a software application targeted towards end-user software clients, available via Cloud. As part of this offering, the CSP will be covering the platform architecture layer which entails development of environments, database management systems, libraries, compilers and other testing tools needed to develop and implement the applications. Additionally, the CSP will be providing the physical infrastructure layer which typically includes the facility layer (heating, ventilation, air conditioning, power, etc.) and the hardware layer (servers, storage, network components, etc.) as well as the virtualized infrastructure layer which includes software elements (hypervisors, virtual machines, virtual data storage), used to realize the infrastructure upon which a Cloud computing platform can be established.

Similarly, the Platform as a Service (PaaS) model covers the platform architecture layers as well as the infrastructure layer, both the physical and the virtualized one. While for Infrastructure as a Service (IaaS), the CSP will be providing the virtualized and the physical infrastructure layers.

Deployment Models

Cloud computing has three primary deployment models, with most of the countries adopting a composition of these three (refer to Figure 2). Each of these deployment models can offer the different service models explained above, the main difference lies primarily in the level of control and ownership the CSP assumes versus the ownership of the user (consumer).



	Private Cloud	Community Cloud *(e.g. Government owned)*	Public Cloud
Users	Used by a **single organization** (e.g. one ministry)	Used by **community of consumers** (e.g. Government ministries)	Used by the **general public**
Operating model	Owned and operated by **the organization itself,** a **third party** or **a combination** of both	Owned and operated by **one or more organizations of the community or** a **third party**	Owned and operated by a **business (local/international), Government, academic organization**
Location	May exist **on or off premises**	May exist **on or off premises**	**Exists on the premises** of the Cloud provider
SLA/Uptime	**No guarantees**, data redundancy is self managed	**Guaranteed by provider**, data redundancy is managed by provider	**Guaranteed by provider**, data redundancy is managed by provider
Timeline	**Longer timelines**, due to deployment & testing	**Faster timelines,** plug and play model	**Faster timelines,** plug and play model
Example	Private Cloud of **USA Ministry of Defense**	**KSA's National Information Center, Singapore's Gov-Cloud**	**AWS, Google Cloud, Singtel, STC, SITCO**

Hybrid Cloud – *Combination of the above three models*

Figure 2 - Cloud computing deployment models

Private Cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising of multiple users (e.g. business units). It may be owned, managed, and operated by the organization, a third party (e.g. a CSP), or a combination of these. The physical location may be on or off premise. There are no guarantees on SLAs/Uptime and data redundancy is managed by the entity itself. Solutions development on private Clouds typically consume more time as all the deployment and testing needs to be done in-house.

Common examples of a private Cloud for Governmental sector are the entity's own Clouds, that are typically serving the entity or an exclusive collection of entities.

Community Cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared/aligned interests (e.g., mission, cyber 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 a combination of these. The physical location may be on or off premise. The SLAs/Uptime are guaranteed by the service provider and the data redundancy is managed by the provider as well. This model offers a "plug and play" model which allows for faster timelines for deployment of new solutions.

A common form of community Cloud for the Public sector is a Government-owned community Cloud, which is often cited as "G-Cloud" or "Gov-Cloud". This is a Cloud typically fully owned by a Government, and provisioned for the exclusive use of Governmental entities. Operations for this Cloud could be done by a Governmental entity, a third party (e.g. a CSP) or a combination of these. It is typically located inside the country, mainly to protect data sovereignty.

In the context of KSA, this Government owned community Cloud will be established and operated mainly by the National Information Center (NIC).

Public Cloud: The cloud infrastructure is provisioned for open use by a variety of entities. It may be owned, managed, and operated by a business, academic, or government organization, or a combination of these. It exists on the premises of the cloud provider. Public Cloud is typically served by global players (e.g. AWS, Google Cloud, Microsoft Azure) as well as by local players (e.g. local telecom and ICT players). The SLAs/Uptime are guaranteed by the service provider and the data redundancy is managed by the provider as well. This model offers a "plug and play" model which allows for faster timelines for deployment of new solutions.

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). A multi-Cloud approach, a similar model, is a composition of two or more distinct cloud infrastructures but without necessarily connectivity or orchestration between them. Such approach is globally endorsed.

Introduction to Cloud First Policy

A Cloud First Policy is a policy meant to define and typically stimulate Public sector migration from traditional IT solutions to Cloud-based models.

How Cloud computing helps the public sector

Globally, multiple Governments have been adopting Cloud computing. This is mainly to benefit from advantages Cloud computing bears, particularly in terms of efficiency improvements, enhanced agility, reliability of services, more robust cyber security and increased innovation.

Efficiency improvement: In its essence, Cloud computing is about resource pooling and sharing across different applications and entities, leading to an increased utilization of the assets. This increase in utilization means that more value is derived from the assets, which optimizes the current state and reduces the need for future capacity expansions, which translates into cost effectiveness.

Migration of infrastructure to Cloud typically results in ~30% savings in terms of total cost of ownership[2]. Additionally, Cloud computing serves as a catalyst which can accelerate the implementation of Data Center Consolidation initiatives. Similar efficiencies can be seen in applications and platforms, particularly when taking the aggregation of demand that will occur into consideration. This aggregation helps streamline the demand, removes duplications and realizes synergies from scale. In summary, Cloud computing will help entities to shift focus from technology itself to higher-value added activities, while focusing on its core competencies and on the mission of the entity.

Enhanced agility and reliability: By leveraging scalability of Cloud computing, entities are typically able to improve services' responsiveness, particularly in cases of fluctuating demand. Unlike traditional IT which is typically built upon a fixed capacity against a forecasted demand, Cloud solutions offer the users the flexibility to scale up and scale down depending on the demand, which improves the overall user experience with minimal additional investments required while minimizing the service disruptions and outages that could occur. Additionally, Cloud computing – through its dynamic and streamlined approach – will help end users improve the overall time to market. For example, while traditional IT solutions would typically require an elongated period to take care of the development, integration, testing and implementation, a commercially available Cloud solution typically serves the same purpose with a "plug and play" approach. Cloud computing provides a more interoperable and portable environment for data and systems that would help achieve seamless communication between the different entities.

More robust cyber security: Beyond achieving a more efficient, innovative and agile environment, Cloud computing helps to improve overall cyber security. By following best-in-class cyber security protocols in the network communication, Cloud services typically offer a high level of cyber security that is difficult to be attained by Governmental entities themselves. In fact, leading Cloud Service Providers have shown to invest significantly into cyber security-related R&D activities[3]. But human errors in the settings remain in the cloud computing, so it is recommended that the employees of cloud computing platforms in the government and commercial government be qualified Saudis and that the hosting is in the Kingdom without the ability to access it remotely from outside the Kingdom.

[2] According to Gartner.

[3] According to Reuters report, Microsoft to continue to invest $1bn a year on R&D for Cyber Security.

Increased innovation: Cloud computing is by nature a driver of innovation for the whole ecosystem. This innovation covers the primary scope of Cloud solutions (infrastructure, platform, software) and is an enabler to transform the way Governmental entities deploy services.

For example, Cloud has already helped transform several private sectors (the way we order a cab, the way we order food, communication with other people, meetings, etc.), all are now online and available anytime anywhere with a simple connection to the internet. It is inevitable that this knowledge and past successful experiences of Cloud computing will be transferred into Governmental processes (e.g. e-Government services "Yasser"). In fact, because of limited initial investment, Cloud computing helps Governmental entities adopt the "start small" entrepreneurial approach to investments, which in turn means more willingness to deploy innovative solutions without having to go through several rounds of budget approvals.

In the case of KSA, Cloud computing will help leapfrog efficiency and effectiveness of IT investments in the public sector (as described in Figure 3).

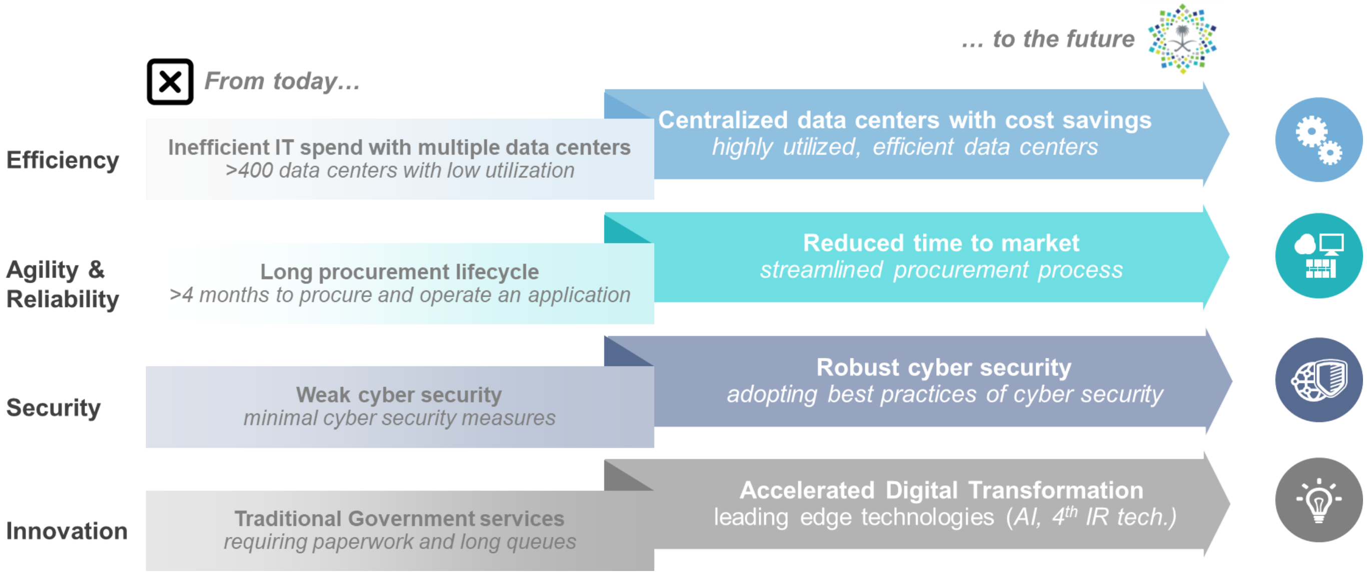

From today…
… to the future
Efficiency
Inefficient IT spend with multiple data centers
>400 data centers with low utilization
Centralized data centers with cost savings
highly utilized, efficient data centers
Agility & Reliability
Long procurement lifecycle
>4 months to procure and operate an application
Reduced time to market
streamlined procurement process
Security
Weak cyber security
minimal cyber security measures
Robust cyber security
adopting best practices of cyber security
Innovation
Traditional Government services
requiring paperwork and long queues
Accelerated Digital Transformation
leading edge technologies (AI, 4th IR tech.)

Figure 3 – Cloud First Policy impact on KSA public sector

Cloud computing will help rationalize Government IT spend. Currently, KSA Government entities have a fragmented IT infrastructure with >400 data centers spread across entities, with a relatively low utilization. Cloud computing will enable a more centralized infrastructure with mega data centers serving all Governmental entities that are highly utilized and more efficient. Entities are now facing major challenges when it comes to procuring IT services (e.g. long procurement cycles). Cloud computing will help reduce the time to market significantly through streamlining the procurement process and adopting a "marketplace" for Cloud services.

In the current set-up, the individual Governmental entities have a responsibility regarding cybersecurity. On the contrary, cloud computing will enable a more coherent and robust cyber security framework through adopting best practices in cyber security across Governmental entities, in which the responsibility of the cybersecurity will be shared between the customers and the CSPs.

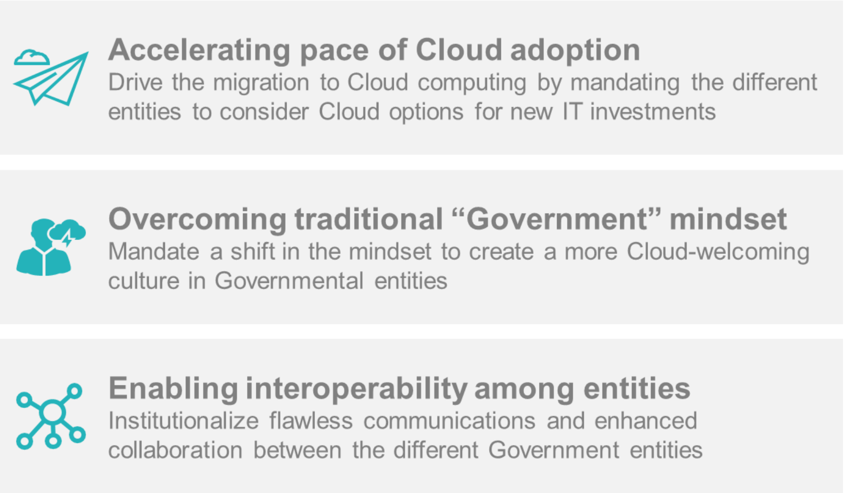
All in all, the impact of Cloud computing will go beyond the Government IT sector, it will accelerate the digital transformation in the Kingdom through pushing adoption of leading edge technologies such as Artificial Intelligence, 4th Industrial Revolution technologies, etc. This will help to increase citizens' satisfaction through innovation of services offered by the Government sector, as Cloud

services will help the Government move from traditional IT services that require more paperwork and longer waiting times, to faster, more automated e-services.
It is recommended to refer to the Cloud Computing Regulatory Framework (CCRF)[4] issued by the Communication and Information Technology Commission (CITC), and any regulation issued or to be issued by the National Cybersecurity Authority to explore more about the regulations governing Cloud computing in KSA and to gain more insights on use cases of Cloud computing for the Government sector.

Implementation of the Cloud First Policy and its benefits

A Cloud First Policy is a policy that covers Governmental entities and aims at accelerating the deployment of Cloud computing services of these entities when making new IT investment decisions. This objective is achieved by mandating these entities to consider Cloud options every time a new IT investment decision is made, in line with the policy guidelines, processes and governance as defined in the Cloud First Policy. The purpose of the policy is to improve efficiency and effectiveness and minimize Total Cost of Ownership of Governmental entities, while enhancing cyber security of information by adopting the right Cloud model for each goal (in line with the data classification laws, policies and regulations of the Government and other relevant regulations). It also enables interoperability and hence improved communication between participating entities.

Multiple Governments of leading countries have opted for a Cloud First Policy aiming for different variations of the objectives as mentioned above. The reasons why these countries put a Cloud First Policy in place are detailed further in Figure 4 and could be summarized as follows:



Accelerating pace of Cloud adoption
Drive the migration to Cloud computing by mandating the different entities to consider Cloud options for new IT investments

Overcoming traditional "Government" mindset
Mandate a shift in the mindset to create a more Cloud-welcoming culture in Governmental entities

Enabling interoperability among entities
Institutionalize flawless communications and enhanced collaboration between the different Government entities

Figure 4 – Reasons why countries adopt a Cloud First Policy

- Accelerated pace of Cloud adoption in the Public sector, by mandating the Governmental entities to consider Cloud options for new IT investments. Countries which have adopted the policy have seen a significant growth of the share of Cloud spend in their Governmental IT spend.
- Overcome traditional "Government" mindset and create a more Cloud-welcoming culture in Governmental entities. In most of the countries, Governmental entities tend to have the

[4] http://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx

preference to deploy their own infrastructure and build their own "customized" applications, a mentality which typically shifts after the introduction of a Cloud First Policy.

- Institutionalize interoperability amongst entities by enabling communications and enhancing collaboration between Government entities.

Considerations for Cloud First Policy

Potential government investments in Cloud computing for the public sector should be evaluated on a case by case basis. Each case should be assessed from 1) a cybersecurity perspective to make sure it satisfies the national cyber security requirements, 2) a technical perspective to ensure its technical viability and 3) a commercial perspective to ensure it represents the most cost-efficient solution available.

A Government Cloud Service Provider is a) a government owned community cloud (NIC) or b) any commercial cloud service provider (global or local) that meets NCA's cybersecurity requirements to host all 4 levels of data classifications (Open, Restricted, Secure and Top Secure). A Commercial Governmental Cloud Service Provider is any commercial cloud provider (global or local) that meets the NCA's cybersecurity requirements to host only Open and Restricted data classifications. All data in both the Government Cloud and the Commercial Governmental Cloud should be located geographically inside the borders of Saudi Arabia.

Cyber Security perspective

When considering migration to Cloud services, cyber security is a key aspect for evaluation and is governed by regulations and laws issued by NCA. Therefore, the policy mainly takes into account the input of data security and protection and builds upon it the decision-making tree for the policy. All cyber security regulations issued by the National Cybersecurity Authority must be reviewed when designing or implementing any cloud solutions to ensure their compliance with security controls and requirements.

Commercial perspective

Cloud computing has significant potential in terms of economic benefits to the migrating entities. However, the economic aspect (quantified by the Total Cost of Ownership) needs to be assessed on a case-by-case basis. For example, applications that are highly customized and specific to the end-user may at times be more expensive to migrate to Cloud compared to the 'as-is' situation.

Technical perspective

Another aspect that should be considered when migrating to Cloud is its technical viability. For example, solutions that are highly sensitive to latency may be better off hosted locally on premise, especially when the Cloud services solutions don't present the same technical features.

In summary, every case should be treated separately and should be rigorously evaluated as such, based on the three dimensions highlighted above.

KSA's Cloud First Policy

Given the benefits as highlighted above, the Kingdom of Saudi Arabia has decided to adopt a Cloud First Policy.

Purpose of the policy

This policy is intended to accelerate the pace at which Governmental entities are migrating from traditional IT solutions to Cloud solutions, which will serve as a key pillar in supporting and driving the digital transformation in KSA.

Entities covered by the scope of this policy are required to consider Cloud computing options when making new IT investment decisions, with the goal to achieve the following:

- Increase quality of service by using more agile, innovative solutions in the Government services sector (e-services).
- Reduce total cost of ownership by improving IT utilization, aggregating demand and removing duplications in Governmental IT spend.
- Improve cyber security robustness by using accredited platforms with best-in-class cyber security standards by leveraging Cloud service providers' expertise in this domain.
- Enable interoperability with other entities.

Scope of the policy

This policy is applicable to all Governmental entities with an exception of the Saudi Arabian Monetary Authority and other entities primarily responsible for the national security and defense, such as:

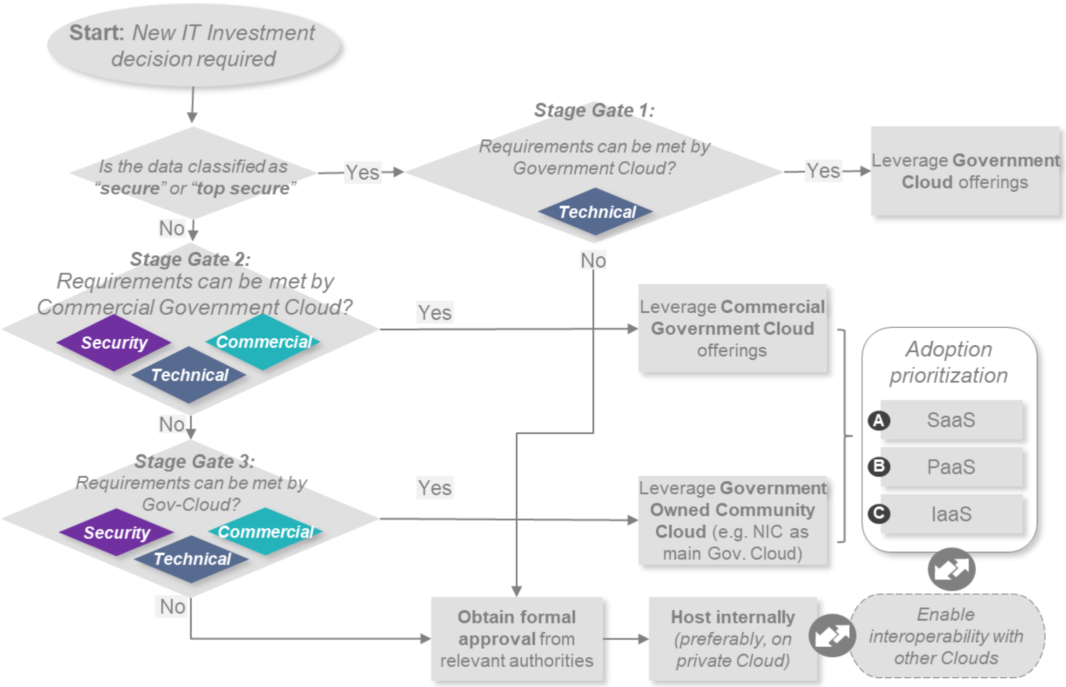
- Ministry of Defense (MoD).
- Presidency of State Security (PSS).
- Ministry of Interior (MoI).
- National Cybersecurity Authority (NCA)

It is also highly recommended for commercially registered entities that are fully or partially owned by the KSA Government[5] as well as the private sector to leverage this policy and create similar internal Cloud First policies for their respective organizations.

Policy's Guidelines

When making new IT investments, entities covered by this policy are required to consider Cloud computing options and must adopt the following multi-faceted approach as illustrated in Figure 5.

[5] Companies/Entities for which KSA Government has 1 or more seats in the board.


Start: New IT Investment decision required
Is the data classified as "secure" or "top secure"
Yes
No
Stage Gate 1:
Requirements can be met by Government Cloud?
Technical
Yes
No
Leverage Government Cloud offerings
Stage Gate 2:
Requirements can be met by Commercial Government Cloud?
Security
Commercial
Technical
Yes
No
Leverage Commercial Government Cloud offerings
Adoption prioritization
A SaaS
B PaaS
C IaaS
Stage Gate 3:
Requirements can be met by Gov-Cloud?
Security
Commercial
Technical
Yes
No
Leverage Government Owned Community Cloud (e.g. NIC as main Gov. Cloud)
Obtain formal approval from relevant authorities
Host internally (preferably, on private Cloud)
Enable interoperability with other Clouds

! Government agencies are not allowed to buy or build new data center infrastructure

Figure 5 – Process to be followed for new IT investments in KSA Government sector

1. **Start**: All new IT investments which are to be made by one of the entities which are included in the scope of the Cloud First Policy need to go through the process. A 'New IT investment' includes procurement of new hardware and software, renewal of hardware and renewal of present software licenses. It is noteworthy that the entities falling under the scope of this policy must abide by the laws, regulations and controls related to data classification and other regulations regarding the location of hosting their data in any way.

2. **Stage Gate 1**: If data is classified in level 1 (top secure) or level 2 (secure), the government cloud service providers (NIC) should be relied upon only if the technical and cybersecurity requirements are met. In the case that the government cloud service providers do not meet the technical and the cybersecurity requirements, the entity can then seek approval from the Cloud computing adoption team[6] to host the software/application internally (preferably a private cloud).

3. **Stage Gate 2:** If data is not classified in level 1 (top secure) or level 2 (secure), entities should utilize the deployment model of Commercial Government Cloud Service Providers only if the security, technical, and commercial requirements are met (assessment process detailed in Figure 6 below) for the goal to maximize value and benefit from optimal costs as well as a diverse range of offerings. With regards to the data classification, data

[6] Further details regarding the approval process of the Government Cloud Office at YESSER will be issued later.

classified in level 3 (restricted) should seek approval from the National Data Management Office, and for data classified in level 4 (open), can be directly used through commercial government cloud service provider under the condition of meeting security, commercial and technical requirements.

4. **Stage Gate 3**: Only if the security, technical, and commercial requirements cannot be met by Commercial Government Cloud Service Providers (assessment process detailed in Figure 6 below), entities should assess solutions from government cloud service provider (NIC) and should adopt this model when requirements are met. For instance, when the National Data Management Office disapproves relying upon the Commercial Government Cloud Service Providers for the data that is classified as (restricted) (for reasons related to the sensitivity of the system to be hosted, for example) , the government cloud should be adopted.

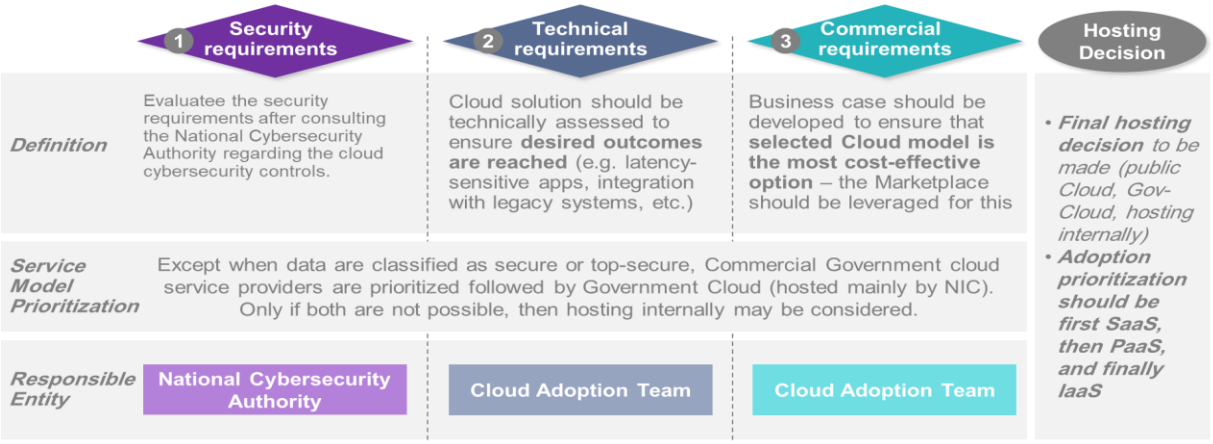
5. Only when the requirements are not met by either Commercial Government Cloud Service Providers or Government Cloud Service Provider, the entity needs then to seek appropriate approvals from the Cloud computing adoption team (refer to Governance section) to deploy an internally hosted solution. If the approval is attained, entities can deploy internal hosting while enabling interoperability with the other Commercial Government Cloud Service Providers and Government owned community cloud in line with the National Enterprise Architecture (NEA) guidelines and requirements applied by Yesser.

   Entities should consider the following priority in terms of service model when selecting a Cloud solution:

   a) Software as a Service (SaaS) is the preferred option as it maximizes the benefits brought by Cloud.
   b) Platform as a Service (PaaS) when SaaS is not possible.
   c) Infrastructure as a Service (IaaS), when SaaS and PaaS are not feasible.

Additionally, with the aim of achieving a more efficient, more utilized IT in the KSA Government sector, entities covered by the scope of this policy are no longer allowed to buy or build new data center infrastructure (e.g. data center, servers or other, storage media, network equipment, uninterruptible power sources).

The exact process that is to be followed (across cyber security, commercial and technical dimensions) in each stage gate is further detailed in Figure 6 below.



	1 Security requirements	2 Technical requirements	3 Commercial requirements	Hosting Decision
Definition	Evaluatee the security requirements after consulting the National Cybersecurity Authority regarding the cloud cybersecurity controls.	Cloud solution should be technically assessed to ensure **desired outcomes are reached** (e.g. latency-sensitive apps, integration with legacy systems, etc.)	Business case should be developed to ensure that **selected Cloud model is the most cost-effective option** – the Marketplace should be leveraged for this	• ***Final hosting decision*** *to be made (public Cloud, Gov-Cloud, hosting internally)* • ***Adoption prioritization should be first SaaS, then PaaS, and finally IaaS***
Service Model Prioritization	Except when data are classified as secure or top-secure, Commercial Government cloud service providers are prioritized followed by Government Cloud (hosted mainly by NIC). Only if both are not possible, then hosting internally may be considered.			
Responsible Entity	National Cybersecurity Authority	Cloud Adoption Team	Cloud Adoption Team	

Figure 6 - Detailed process followed at stage gates

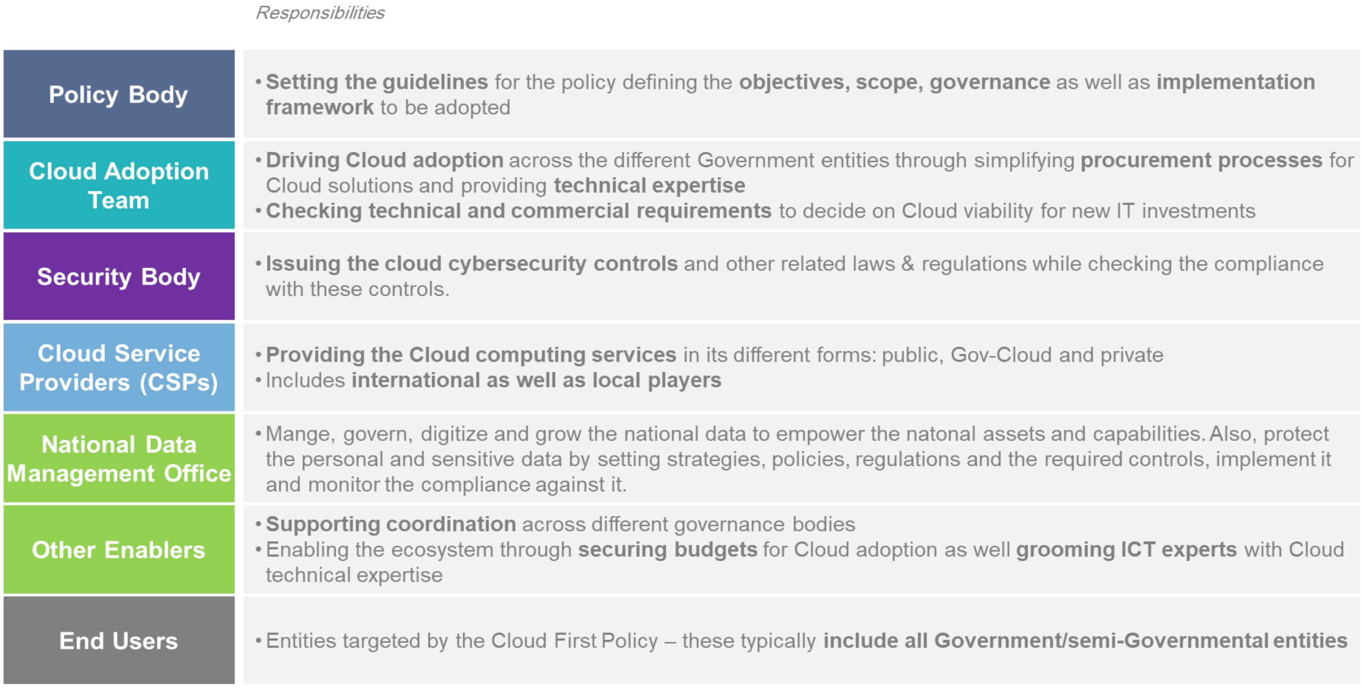
- **Cyber Security requirements**: assess if the cyber security requirements, which are based on the governing data classification law in the KSA, authentication requirements and other specific cyber security measures and regulations, are met by the Cloud model under consideration (Commercial Government Cloud or Government Cloud) while liaising with the assigned Security Body (refer to Governance section). With regards to data classification specifically, the general rule in this policy is data classified in level 1 (top secure) or level 2 (secure) must be hosted in the Government cloud (NIC).And for data that is classified in level 3 (restricted), the National Data Management Office should be asked for approval as the office may decide that the data should be considered in level 1 (top secure) or level 2 (secure) due to its sensitivity or other security considerations). Lastly, data classified in level 4 (open) can directly make use of commercial government cloud service providers.

- **Commercial requirements**: assess the commercial aspect of the Cloud adoption case to ensure that it yields a positive business case, i.e. that the selected Cloud computing model (Commercial Government Cloud or Government owned community Cloud) offers the most cost-effective option for each specific case. This should be done in coordination with the Cloud computing adoption team (refer to Governance section).

- **Technical requirements**: assess the technical aspect of the Cloud migration case, to ensure that the Cloud solution will achieve the desired outcomes (e.g. for cases of latency-sensitive applications, integration with legacy systems, etc.). This should be done in coordination with the Cloud computing adoption team (refer to Governance section).

Governance Structure

A well-defined governance structure must be in place to ensure smooth implementation and optimal results. There are six main roles defined to govern the implementation of the Cloud First Policy (refer to figure 7).



	Responsibilities
Policy Body	• **Setting the guidelines** for the policy defining the **objectives, scope, governance** as well as **implementation framework** to be adopted
Cloud Adoption Team	• **Driving Cloud adoption** across the different Government entities through simplifying **procurement processes** for Cloud solutions and providing **technical expertise** • **Checking technical and commercial requirements** to decide on Cloud viability for new IT investments
Security Body	• **Issuing the cloud cybersecurity controls** and other related laws & regulations while checking the compliance with these controls.
Cloud Service Providers (CSPs)	• **Providing the Cloud computing services** in its different forms: public, Gov-Cloud and private • Includes **international as well as local players**
National Data Management Office	• Mange, govern, digitize and grow the national data to empower the natonal assets and capabilities. Also, protect the personal and sensitive data by setting strategies, policies, regulations and the required controls, implement it and monitor the compliance against it.
Other Enablers	• **Supporting coordination** across different governance bodies • Enabling the ecosystem through **securing budgets** for Cloud adoption as well **grooming ICT experts** with Cloud technical expertise
End Users	• Entities targeted by the Cloud First Policy – these typically **include all Government/semi-Governmental entities**

Figure 7 – Governance structure for Cloud First Policy

In case of the Kingdom of Saudi Arabia, the roles and responsibilities to successfully implement this Cloud First Policy are illustrated in Figure 8.

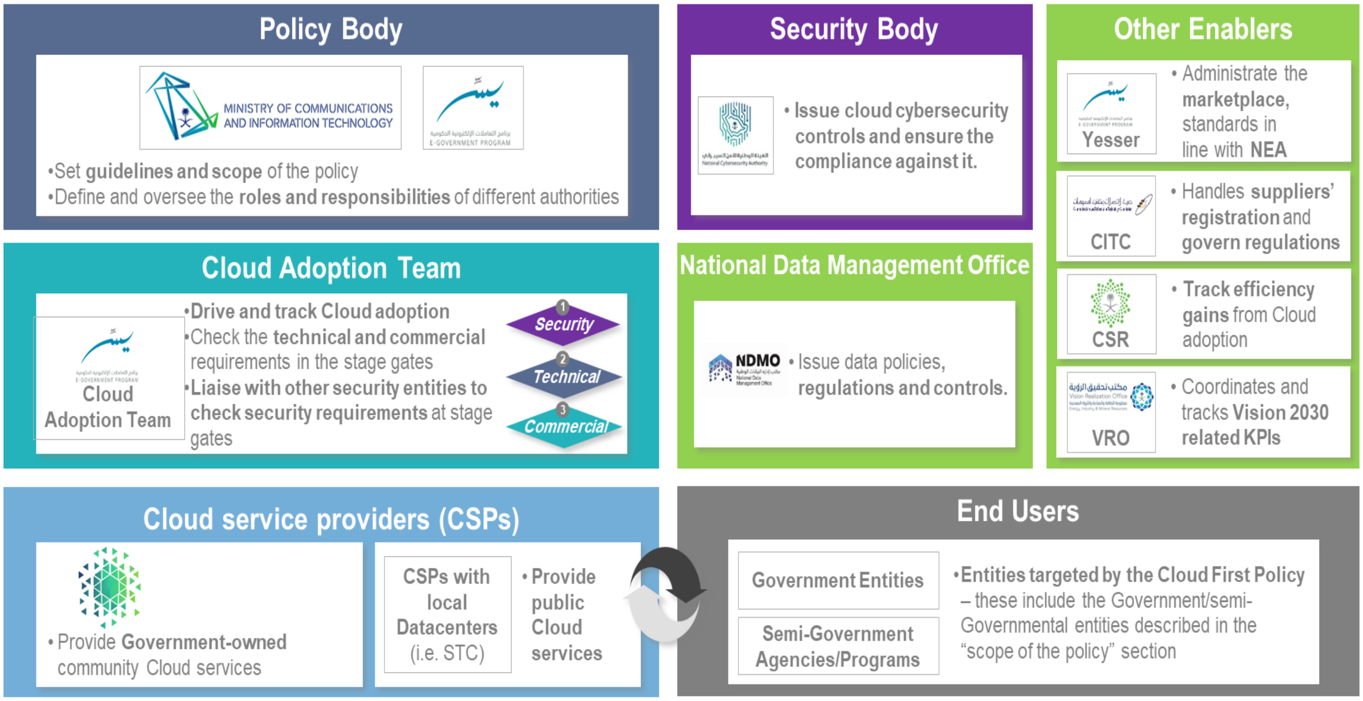

Policy Body
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
E-GOVERNMENT PROGRAM
•Set guidelines and scope of the policy
•Define and oversee the roles and responsibilities of different authorities
Security Body
• Issue cloud cybersecurity controls and ensure the compliance against it.
Other Enablers
Yesser
• Administrate the marketplace, standards in line with NEA
CITC
• Handles suppliers' registration and govern regulations
CSR
• Track efficiency gains from Cloud adoption
VRO
• Coordinates and tracks Vision 2030 related KPIs
Cloud Adoption Team
Cloud Adoption Team
•Drive and track Cloud adoption
•Check the technical and commercial requirements in the stage gates
•Liaise with other security entities to check security requirements at stage gates
1 Security
2 Technical
3 Commercial
National Data Management Office
NDMO
• Issue data policies, regulations and controls.
Cloud service providers (CSPs)
• Provide Government-owned community Cloud services
CSPs with local Datacenters (i.e. STC)
• Provide public Cloud services
End Users
Government Entities
Semi-Government Agencies/Programs
•Entities targeted by the Cloud First Policy – these include the Government/semi-Governmental entities described in the "scope of the policy" section

Figure 8 - Governance structure for Cloud First Policy in KSA

Policy Body

1. Ministry of Communications and Information Technology (MCIT).
   a. Defining the objectives and scope of the Cloud First Policy.
   b. Setting the guidelines for the policy and publishing these.
   c. Defining the roles and responsibilities of the different involved entities, in the context of the Cloud First Policy.
   d. Updating and adjusting the Cloud First Policy when required.
2. Yesser
   a. Supporting MCIT in the definition of the objectives and scope of the Cloud First Policy.
   b. Establishing governance structure for the Cloud First Policy.

Cloud Computing Adoption Team (CCAT)

3. Cloud computing adoption team in the government - Yesser.
   a. Driving the Cloud across the different Governmental entities though pilots and supporting entities during the migration process with technical and commercial expertise.
   b. Liaising with Ministry of Finance – Center of Spending Rationalization (CSR) to secure budgets for Cloud projects.
   c. Checking the cybersecurity, technical and commercial requirements at the Stage Gates.
   d. Handling accreditation of Cloud services offered to the Government sector.
   e. Tracking the adoption progress and producing nation-wide progress dashboards across selected key performance indicators (KPIs)

National Data Management Office

4. Data Office(s).
   a. Establish data classification policy, enable its application and ensure compliance with it.

Security Body

5. National Cyber Security Authority (NCA).
    a. Issuing the cloud cybersecurity controls and other related regulations and verifying compliance with it.

Enablers

6. Yesser
    a. Administrating the Marketplace that will connect Cloud suppliers with the buyers.
    b. Streamlining the procurement process for Cloud solutions.
    c. Supporting entities in migration by providing technical and commercial expertise.
    d. Ensuring standards and interoperability compliance in line with National Enterprise Architecture (NEA).
7. Center of Spending Rationalization (CSR)
    a. Identifying the Cloud adoption opportunities.
    b. Supporting the Cloud computing adoption team with key financial information when required.
    c. Aiding the Cloud computing adoption team in providing incentives if necessary.
8. Vision Realization Office (VRO)
    a. Supporting in the coordination of Vision 2030 relevant KPIs to the different responsible entities.
    b. Tracking and overseeing of these relevant KPIs.
9. Communications and Information Technology Commission (CITC)
    a. Handling the Cloud Service Providers' (CSP) registration in line with the Cloud Computing Regulatory Framework (CCRF).
    b. Governing the regulatory environment for Cloud computing.

Cloud Service Providers

10. National Information Center (NIC)
    a. Providing the Government-Cloud services to the entities.
    b. Supporting entities to better understand the Cloud offerings of the Government-Cloud.
11. Cloud Service Providers (CSPs)
    a. Providing public Cloud services to the entities.
    b. Supporting entities to better understand the Cloud offerings of the public Cloud.

End Users

12. Government entities
    a. All entities as defined in 'Scope of the policy' section.
    b. These entities are buyers of Cloud services.

All the entities mentioned above will ensure continuous and transparent collaboration to drive the Cloud adoption in the Government sector in KSA.

A high-level implementation/ enforcement plan will be detailed further as part of the Nation's Cloud strategy. This plan will include the main initiatives the Government will be implementing in its aim to drive Cloud adoption (including audit mechanism, pilot programs, etc.). It is in favor of the Kingdom of Saudi Arabia to rationalize the spend on IT and to reinvest the savings in high-value added activities.

Appendix

List of definitions

Below is a list of the definitions of key terms used in the above policy document.

Term	Definition
Cloud First Policy	A policy that mandates public sector entities to consider Cloud options when making new IT investment decisions.
Cloud Computing Regulatory Framework (CCRF)	A framework published by the Communication and Information Technology Commission (CITC) and aiming at providing increased regulatory clarity regarding Cloud services in KSA.
Cloud Computing	A model which enables 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.
Cloud Service Provider	Entities providing Cloud Services to the public either directly or indirectly, such as a Cloud Provider, Cloud Broker, Cloud Aggregator, reseller or agent of a Cloud Provider, whereby Cloud Service Providers are only allowed to operate and offers services in KSA if they are registered with Communication and Information Technology Commission (CITC) as per the Cloud Computing Regulatory Framework (CCRF).
Governmental Entity	Public sector entities that are fully controlled by the Government. These include but are not limited to, ministries, universities, councils, etc.
A Government Cloud Service Provider	a) A government owned community cloud (i.e. NIC) or b) any commercial cloud service provider (global or local) that meets NCA's cybersecurity requirements to host all 4 levels of data classifications (Open, Restricted, Secure and Top Secure).
A Commercial Governmental Cloud Service Provider	Any commercial cloud provider (global or local) that meets the NCA's cybersecurity requirements to host only Open and Restricted data classifications
Stage Gate	A decision point at which requirements (security, commercial and technical in this case) are checked to decide on what is the best suitable outcome for each case.
Latency sensitive	Latency is defined as the time between the occurrence of an event and its handling. Latency sensitive applications are those that need to react "fast" to specific events and that internet disruptions and delays would cause huge disruption in their operations.
Legacy systems	Computer system, technology and application program that are old and outdated, in the case of Cloud computing, these are systems that very difficult be connected and hosted on Cloud in their as-is state.
Interoperability	Ability of several systems, business units or entities to exchange data seamlessly between each other and to use this data in the operations.
New IT Investment	Includes procurement of new hardware and software within any amount, as well as renewal of hardware and renewal of software licenses (as described in the policy guidelines).
Public Sector	The part of the economy which is controlled by the Government.
Private Sector	The part of the national economy that is not controlled by the Government, this includes but is not limited to large, medium and small enterprises as well as new startups and entrepreneurships.

List of abbreviations

Below is a list of the abbreviations of key terms used in the above policy document.

Acronym	Meaning
CSP	Cloud Service Provider
CCRF	Cloud Computing Regulatory Framework
PC	Personal Computer
IT	Information Technology
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
NIST	National Institute of Standards and Technology
AWS	Amazon Web Services
ICT	Information, Communications and Technology
R&D	Research & Development
4th IR	Fourth Industrial Revolution
AI	Artificial Intelligence
CITC	Communications and Information Technology Commission
MoD	Ministry of Defense
PSS	Presidency of State Security
NEA	National Enterprise Architecture
NCA	National Cyber Security Authority
NIC	National Information Center
CSR	Center of Spending Rationalization
VRO	Vision Realization Office