Ministry of Information Technology
& Telecommunication

DIGITAL PAKISTAN

PAKISTAN CLOUD FIRST POLICY

February 2022

Table of Contents

1 Definitions and Abbreviations

1.1 Cloud Computing

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

1.2 Cloud Service Provider (CSP)

A Cloud Service Provider (CSP) is a third-party company that offers components of cloud computing such as infrastructure, software, storage, application, etc.

1.3 Public Sector Entities (PSE)

The Government of Pakistan (GOP) including all its Ministries, Departments, Agencies, Dependencies, and Institutions at the Federal level; and corporations fully or partially owned by the Federal Government of Pakistan.

1.4 Government data

Data collected, generated, processed and/or managed by Public Sector Entities.

1.5 Interoperability

The ability of computer systems, platforms, software, databases or different computerized products or systems or their components to exchange and use information seamlessly between each other.

1.6 New ICT Investment

Procurement of new ICT hardware and software as well as renewal of hardware and renewal of software licenses.

1.7 Open Data

Publicly available data structured in a way that the data is fully discoverable and usable by end users is called ‘open data’.

1.8 Service Level Agreement (SLA)

An agreement between a customer and a service provider that lists the services required and the expected level / quality / grade of service.

1.9 Abbreviations

ABBREVIATION	MEANING
BVN	Bank Verification Number
CAO	Cloud Acquisition Office
CSP	Cloud Service Provider
GOP	Government of Pakistan
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IT	Information Technology
MoITT	Ministry of Information Technology and Telecommunication
PaaS	Platform as a Service
PCFP	Pakistan Cloud First Policy
PII	Personally Identifiable Information
PPRA	Public Procurement Regulatory Authority
PSE	Public Sector Entities
SaaS	Software as a Service
SDG	Sustainable Development Goals
SLA	Service Level Agreement

2 Background

Cloud computing offers a wide variety of potential benefits and opportunities: reduced costs, improved responsiveness to citizens' needs, increased transparency, environmental benefits & reduced carbon footprint, efficient management, optimization of resources and enhanced public service delivery. Cloud computing fundamentally changes how organizations use Information and Communications Technologies (ICT) in a more efficient way, therefore, all necessary steps are required to be taken to ensure a seamless cloud adoption process, providing the full advantage of the potential and benefits of cloud computing.

With a thorough analysis of the expected benefits of cloud computing, the Ministry of Information Technology and Telecommunication (MoITT) is confident that this technology will bring improved access to the delivery of public services for the benefit of all the citizens of Pakistan and provide efficient means of governance to the Government of Pakistan (GoP). The supporting strategy for cloud implementation and the adoption of a cloud model that best suits the needs of the organization will reduce the time and cost of digital service adoption for public entities. This will provide customers with the flexibility to decide, upon their needs and requirements, which applications, data, and resources can be put in the appropriate cloud service and deployment model.

Therefore, in coordination with relevant authorities and stakeholders, MoITT publishes Pakistan Cloud-First Policy (PCFP) to encourage cloud adoption across Pakistan. This policy aims to guide and empower organizations to transition to cloud-based solutions. Enabling the accelerated cloud adoption for public sector will fast-track the digital transformation journey of Pakistan. It is also expected that the policy will result in cloud adoption across a variety of markets and industries and foster the growth of the local ICT industry by enabling access to cloud-based technologies and complementing emerging technologies such as Artificial Intelligence, Machine Learning, and the Internet of Things. This will also provide an opportunity for the indigenous industry to benefit from local and global cloud demand and develop, deploy and market services and solutions based on various cloud service delivery models. Cloud adoption in public sector of Pakistan will also enable GoP to utilize latest technological solutions available in the ever-evolving ICT industry.

PCFP is an important element for the achievement of the objectives outlined in the Digital Pakistan Policy such as improving the responsiveness and effectiveness of services delivery by the Government to citizens. It constitutes an integral part to support the GOP's efforts to promote mass adoption of emerging digital technologies, accelerate digital transformation and development of innovative applications to enable cross-sector socio-economic development and transformation of economic activities, governance models, social interaction, and achievement of sustainable development goals (SDG).Through this policy, MoITT aims to contribute to the GOP's goal to promote e-Governance to make Pakistan the frontrunner in good governance through IT enablement at all levels. MoITT also aims to reduce the burden of import bills of Pakistan by discouraging investments in organization specific data centres in Public Sector Organizations (PSE) and taking advantage of the economies of scale offered by the cloud.

MoITT is determined to develop an ongoing and iterative programme of work that will enable the use of a range of cloud solutions as well as change the way ICT is procured and operated, throughout Pakistan. Successful implementation of this policy will require the help and coordinated efforts from different government departments especially by Ministry of Planning, Development & Special Initiatives for not allowing any public investments into projects having fragmented data centre (non-cloud) components, and PPRA for prioritizing cloud adoption by enabling and prioritizing flexible cloud procurement models to integrate cloud capabilities quickly and efficiently and remove obstacles to its adoption. To provide a coherent approach to cloud adoption across Pakistan, provide ease of doing business and to avoid duplication of efforts, support of provincial governments is utmost necessary for the adoption of this policy in their jurisdictions.

The salient takeaways of cloud computing are:

a. Efficient (cost of) governance: Efficient technology resources can be procured on a “pay as you use” basis and is cost-efficient. Resources of a cloud data center are shared among many organizations. Therefore, fewer servers, storage, network equipment and power & cooling equipment are utilized. Furthermore, the frequent purchase of ICT equipment to replace obsolete equipment every few years is also replaced with paying for only the services utilized. This will result in cost efficiency for organizations and will reduce the overall import bill of Pakistan.

b. Information security: CSP hold internationally recognised security certifications that are assessed by third-party security professionals. Information security challenges are adequately addressed via cloud computing by following international standards and best practises

c. Data privacy: CSP implement technical and administrative controls to protect data – both stored and in transit. Furthermore, formal engagements with CSP generally define data protection standards and establish SLA that outline security and privacy measures. These measures including but not limited to adequate technical controls, such as end-to-end encryption or tokenization as well as data loss prevention tools.

d. Transparency and accountability: Cloud computing improves transparency and accountability in the public administration. Likewise, it enables open access to (publicly available) government information and data for governments, citizens, and businesses, leading to increased engagement and participation, as well as fostering trust.

e. Innovation in public sector delivery: Cloud computing accelerates digital transformation through agility and innovation. A variety of tools such as social media, mobile platforms and analytic tools are available to PSE on subscription basis which result in enhancing e-citizen services.

f. Resource optimization: Cloud computing is efficient in resource utilization as compared to segregated data centres because it is based on the concept of sharing services and hence maximizing the effectiveness of resources. An on-premises data center is mostly underutilized. The equipment usually does not do much more than handling routine tasks and stay powered on over the weekends and during off work hours. Whereas in a cloud environment, the unutilized compute cycles of one organization may be used by another organization. Furthermore, it results in optimum utilization of Human Resources as it is easier to manage centralized infrastructure with fewer and highly skilled human resources.

g. Environmental Benefits: Cloud computing reduces energy consumption, waste and carbon emissions. Cloud decreases the rate of carbon emissions by reducing energy requirement and consumption. Cloud adoption means that fewer machines are utilized to serve more users and thus utilizes less energy and have a lower impact on the environment.

3 Vision

This policy envisions digital transformation of Pakistan by optimized ICT spending, efficient utilization of latest cloud-based technologies, swift delivery of citizen services, better governance, increased collaboration among the government organs and enhanced transparency & accountability.

4 Scope and Adoption

PCFP applies to all PSE under the federal government intending to make new ICT investment(s). The PCFP will also serve as useful guidance to regulated sectors and private sector organizations as they continue to undertake digital transformation. PCFP is issued to support the digital transformation of the ICT landscape in Pakistan, improve efficiency, provide quality service delivery, and encourage investments in ICT.

5 Objectives

The government of Pakistan aims to achieve the following objectives with this policy:

a. To reduce time to procure and time to launch by maintaining a pre-accredited list of CSP.
b. To reduce the cost of ICT infrastructure by paying only for the services that are utilized.
c. To encourage investment in cloud services by local and International CSP in Pakistan.
d. To facilitate CSP achieve economies of scale.
e. To provide enhanced information security to end-users via cloud offerings.
f. To provide transparency to citizens with digital government solutions.
g. To increase utilization of cloud solutions by transitioning from local hosting to cloud hosting.
h. To foster a digital entrepreneurship ecosystem by providing readily available cloud services.
i. To attain optimization via aggregation of resources.
j. To develop a cloud enabled workforce.
k. To obtain environmental benefits achieved by optimized use of resources.
l. To put forward a synchronized approach to ICT procurement across the governments/provinces.

6 Current State of Cloud Computing in Pakistan

6.1 Current ICT Infrastructure landscape

Distributed infrastructure which is available in small clusters is difficult to manage. Estimating and planning for the future expansion in a fragmented infrastructure is a challenging task. There is a dire need to have a consolidated infrastructure for PSE in Pakistan. Currently, the utilization of cloud services in the public sector is low and majority of the data centres cater for the need of a single organization only. Cloud offers better security and optimization of resources, whether in terms of personnel or compute, storage or network utilization, which cannot be achieved in a fragmented ICT infrastructure

6.2 Human Resources

With the adoption of cloud solutions, certain data centre roles are replaced with domain skills for process automation, resource optimization, architecture, and cost management. One of the objectives of this policy is the development of a skilled cloud-enabled workforce to foster cloud adoption and implementation throughout Pakistan. PSE will be facilitated to ramp up the skills of their existing IT personnel and transform them into a cloud-enabled workforce. Moreover, with the increased demand for cloud technologies, skills, training and development of relevant quality human resources is critical. Special initiatives for the training and up-skilling of the workforce will be prioritised for accelerated cloud adoption.

6.3 Cloud Opportunities in Pakistan

Pakistan is the 5th most populous country in the world with a population of approximately 220 million. The federal government of Pakistan comprises of more than 40 divisions and more than 600 affiliated departments. Similarly, there are numerous provincial ministries and their affiliated departments in all the provinces of Pakistan . The governments across the globe are increasing their spending on ICT to provide better citizen centric services and increased transparency and accountability. Pakistan is undergoing a digital revolution and has taken numerous initiatives for the provisioning of ICT based solutions. This represents a huge potential for investors to offer cloud-based infrastructure and solutions to GoP. This policy aims to provide a conducive environment to CSP to be a partner of the GoP in its digital transformation journey.

7 Cloud Deployment Models

7.1 Public Cloud

- Cloud infrastructure provisioned for open use by the general public.
- This cloud model may be owned, managed, and operated by a business, academic, or PSE, or some combination of them.
- It can be located anywhere. Resources of the cloud infrastructure can be shared by any number of organizations.

7.2 Government Cloud

- Cloud infrastructure provisioned for use by PSE only.
- It may be owned, managed, and operated by a business, academic, or PSE, or some combination of them.
- It can only be located in Pakistan. Resources of the cloud infrastructure can be shared by PSE only.

7.3 Private Cloud

- Cloud infrastructure provisioned for exclusive use by a single organisation/PSE.
- It is managed and operated by the organisation, a third party, or some combination of them.
- It can only be located in Pakistan either on premise or off premise of the organization that owns it.

7.4 Hybrid Cloud

- Hybrid cloud is a solution that combines one or more referred cloud deployment models.
- It allows data and applications to be shared between the referred models. An organization can store its sensitive data on one type of cloud whereas public data on another, thus taking care of its security needs as well as leveraging the robust computational resources of a public cloud.

8 Data Sovereignty and Data Flows

This policy acknowledges the capabilities and economies of scale obtained when there are no data residency requirements in place. CSP are hyper-scale providers and have data centres around the world.

The clients usually have the option to restrict their data to a particular geographic region. With no data residency requirement in place, the data belonging to GOP may be stored outside the boundaries of Pakistan and there is a possibility that GOP loses access to its data or the data may be subject to the laws of other countries. However, whenever there are legitimate use-cases requiring cross-border data flows, then the relevant stakeholders may consult with the Cloud Office to ensure appropriate security standards and controls are in place for such data flows.

9 Policy Deliverables

9.1 Cloud Office

A mandated and defined governance structure ensures smooth implementation and optimal operations of cloud services through a dedicated office(s). For the accelerated implementation of this policy, MoITT will set up a dedicated office to facilitate and supervise the matters connected thereto. This office will act as the flag bearer for cloud adoption in Pakistan and will define the criteria for the accreditation/registration of CSP according to domestic and international standards and support provinces in their cloud adoption efforts to bring uniformity in cloud adoption across Pakistan.

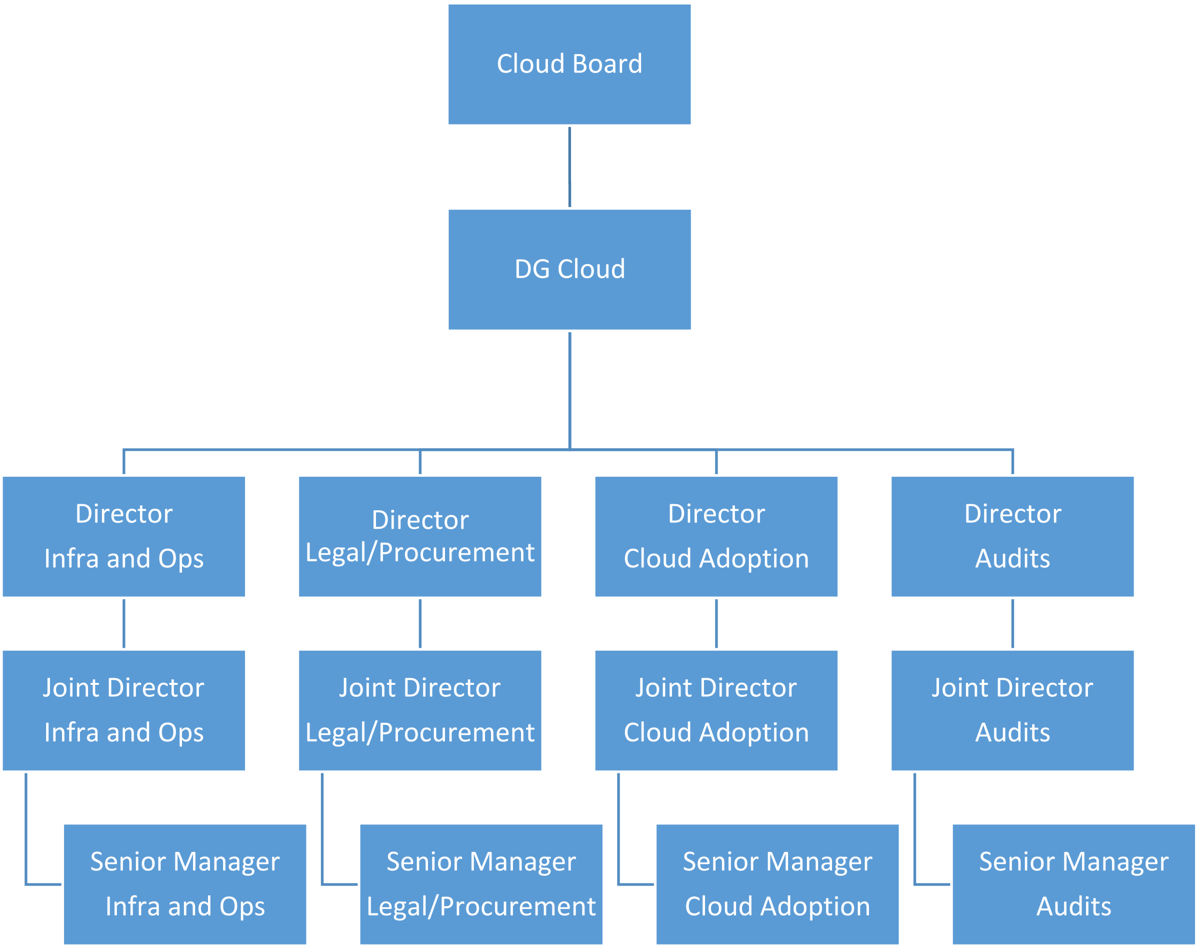
GOP will ensure the implementation of this policy through Cloud Office(s). This planned governance structure will enable the roadmap for establishing a structured and formal organizational setup for cloud governance in Pakistan. Cloud Office is mandated to carry out the following functions

i. Establish a classification, accreditation, registration and compliance framework for CSP based on international benchmarks.
ii. Carry out or seek compliance from the CSP against established benchmarks.
iii. Promote a cloud culture and adoption of cloud services across PSE.
iv. Provide a time-based No Objection Certificate (NOC) if there is a legitimate reason for deviation/exemption to PCFP.
v. Enforcement of modalities for cloud first investments.
vi. Support provinces in adoption of cloud first policy in their jurisdictions.

Annex-A: Cloud Service Models
Annex-B: Priority of Cloud Service Models
Annex-C: Share of Responsibility

9.1.1 Organizational Hierarchy of the Cloud Office

Cloud board will be headed by Secretary MOITT, Government of Pakistan, while Chief Secretaries of all provinces or their representatives and two industry experts will be members of the board. The chief secretaries or their representatives will become part of the Cloud Board as members once respective provincial government adopts cloud first policy in line with this policy.


Cloud Board
DG Cloud
Director Infra and Ops
Director Legal/Procurement
Director Cloud Adoption
Director Audits
Joint Director Infra and Ops
Joint Director Legal/Procurement
Joint Director Cloud Adoption
Joint Director Audits
Senior Manager Infra and Ops
Senior Manager Legal/Procurement
Senior Manager Cloud Adoption
Senior Manager Audits

9.2 Accreditation of Cloud Service Providers for Government Data

CSP will meet domestic and international standards set for accreditation of CSP to fulfil accreditation requirements of the Cloud Office. The Cloud Office will formulate accreditation criteria and benchmarks for all CSP opting to provide services to PSE. The criteria will be based on international benchmarks such as security, reliability, cost, interoperability, availability and any other established parameters. The process for CSP to be listed in the accredited list will be laid out by the Cloud Office.

The Cloud Office will maintain an accredited list of CSP for PSE. This will not only ensure that security and reliability offered by CSP are in compliance with domestic and international standards but will also make the procurement of cloud services easier for PSE. PSE are required to provision services from accredited list of CSP only. The Cloud Office will have the authority to revoke the accreditation of CSP in case of non-compliance.

9.3 Registration of Cloud Service Providers

CSP that intend to host Open Data (Annex-E) are required to get registered with Cloud Office with minimal registration requirements to ensure provision of quality cloud services. Cloud Office will prioritise the ease of doing business for CSP and ensure business enabling environment for cloud adoption.

9.4 ICT Audits

Audits are means to ensure that CSP provide adequate levels of protection for the treatment of information assets in accordance with the standards set by the Cloud Office. This policy mandates that CSP provide satisfactory audit reports or respond to audit requests made by the Cloud Office. Relevant authorities and other certified third parties will be able to monitor and perform audits to validate the contractually agreed controls. Moreover, the CSP should also employ internal audit mechanisms to ensure the prescribed requirements are adhered to. Audits can either be carried out at regular intervals or on as the need be. The Cloud Office can designate any auditing body to carry out the audits based on the criteria outlined by the Cloud Office.

9.5 Cloud Acquisition Office

A Cloud Acquisition Office (CAO) will be established in the federal jurisdiction. Similarly, the province that adopts Cloud Policy in line with this policy will establish CAO in their jurisdictions to support provincial PSE in their transition to the cloud. CAO will facilitate PSE in designing, architecting, procuring, building, migrating, and managing their workloads and applications on the cloud. CAO will initiate call offs for the requirements of PSE. Only CSP accredited by the Cloud Office will be eligible to take part in call offs. CSP with the most advantageous offering will be selected in the call off. SLA will be signed between the CSP and PSE accordingly. Any breach of the SLA between PSE and CSP will be reported to CAO by the PSE. CAO will report continued serious non-compliance of SLA by CSP to Cloud Office. Apart from other remedies available to PSE, the Cloud Office will take appropriate action depending upon the nature and seriousness of non-compliance.

9.6 Restrictions on Investments in Fragmented ICT infrastructure

With the approval of this policy GoP will require all PSE to review any projects which involve setting up a data center/ICT infrastructure/Server Room and will prioritise cloud-based solutions for any future ICT investments. Same provisions will apply on any projects in the public sector implemented via a third-party or donor agency. Federal Government will also advise provincial governments to share the same directives to its subordinate organizations to restrict investments on fragment ICT infrastructure and prioritise cloud. After 1st July 2022, all new ICT investments should adhere to the directions of Cloud Office.

9.7 Data Classification

Data classification is the process of organizing data into categories so that the data can be utilized according to its sensitivity and criticality. PSE will have different types of information and that information will be associated with varying levels of sensitivity. Data classification framework provides a tool to classify and categorize data based on respective sensitivities and hence enable PSE to define controls against each classification category.

A clear data classification framework is essential to ensure that the critical benefits of cloud computing are achieved cost-effectively. This ultimately enables decision-makers to better understand what types of data can be stored on each type of cloud model. Such a framework can be used when considering any type of cloud service as this will allow PSE to better align costs for bespoke security technology for a subset of highly sensitive information that requires such protection and different security for products or services for other less sensitive information. The data can be classified by PSE as outlined by the Government of Pakistan and the guidelines issued by the Cloud Office in this regard.

Annex-D: Data Classification Guidelines
Annex-E: Cloud Selection Matrix

9.8 Security Framework

Information Security is a set of practices to keep the data secure from unauthorized access, alterations, disclosure, disruption, or destruction whether the data is at rest, in motion or in processing. It is intended to ensure confidentiality, integrity, and security of the data.

In a traditional data center, the organization itself is responsible for security across the entire operating environment. In a cloud environment, the security of the contracted cloud solution is shared between the contracting organization and the CSP. Each party maintains complete control over the assets, processes, and functions they own. The responsibilities of each party vary depending on the services procured and how those services are integrated into the overall environment. Both parties should ensure that the confidentiality, integrity, and availability of the data is maintained in this shared responsibility model. The use of any cloud service must remain compliant with applicable laws and regulations of Pakistan.

Data classification is often designed together with information security requirements that are appropriate for managing each level of information. The cloud model that hosts the classified data must meet security requirements for that model. This policy mandates the Cloud Office to define security baselines, based on domestic and international standards, for different cloud models designated to host different data classes for PSE. The CSP and the PSE must maintain utmost integrity to protect the data and meet the security requirements set forth by the Cloud Office and/or any other relevant authority. The failure to satisfy any of the liabilities or obligations shall constitute a breach. Any data breach must be disclosed to the Cloud Office and any other relevant authorities as soon as the breach is discovered. Cloud Office and/or other relevant authorities, as determined in applicable regulations, may seek incident reports and determine appropriate response measures.

In addition to meeting baseline security standards, audits and security monitoring mechanisms must be in place to ensure cloud services meet the data integrity, confidentiality requirements and that there have been no data breaches, and that the data and workloads are continuously available.

10 Procurement

Government procurement is a very relevant aspect of the development of cloud computing. PSE must consider cloud services for all of their new ICT procurement decisions. Any new ICT procurement decision to select services except cloud must have approval by the Cloud Office. Moreover, PSE will also seek approval from Cloud Office to host data on private cloud and will have to demonstrate the need for hosting on private cloud. Similarly, an organization intending to establish its own Private Cloud must have approval of the Cloud Office.

Upon the government approval of this policy, the selection of cloud-based ICT will be prioritized in new ICT procurement. This will apply to infrastructure, hardware, software, information security, licensing, storage, and provision of data, as well as services like security, development, virtualisation, databases, or any kind of technology where a cloud-based offer is essentially equivalent to or better than other kinds of technological solutions.

PSE will consider cloud solutions as the preferred option. To this effect, any decision to not use cloud solutions first must be substantiated by a business case and clear evidence of the value of such a decision. In this regard, the PSE must establish that the non-cloud-based ICT deployment strategy has a lower Total Cost of Ownership (TCO) with at least the same level of security that a cloud deployment offers or it meets special requirements of the PSE that are not offered by a cloud deployment. The selection of the appropriate cloud deployment and service model will be based on an assessment of each application, incorporating cost-benefit analysis and achieving value for money over the life of the investment. Procurement practices should reflect purchasing practices and contract terms that allow cloud platforms to be scalable, cost-effective, and innovative. CAO will facilitate PSE in their selection of the appropriate cloud service and deployment model, architecting, procuring, building, migrating, and managing their workloads and applications on the cloud. CAO will also hold call offs for the selection of accredited CSP.

The following aspects will be considered when procuring cloud services:

a. Value for money-to fulfil the intended purpose of the service;
b. Transitioning from capital budgets to operational expenditure;
c. Short, medium, and long terms impact on finances, governance, technology, relevance, suitability;
d. The suitability of Service Level Agreements in relation to PSE needs; and
e. Information on data security guidelines and compliance with national legislation and international standards on data privacy and cybersecurity;

In general, cloud services are provisioned on a “pay as you use” basis. The organizations requiring ICT services do not have to purchase equipment to obtain services. This is a shift from the traditional way of procuring ICT in public sector in Pakistan which is based on purchasing equipment and incurring a capital expenditure. In order to achieve the goals of PCFP, a new perspective for purchasing and operating ICT will be considered. The “Pay As You Use” and “Self Service” approaches permit scaling of services and is useful as the data and compute needs of an agency fluctuate.

After the approval of this policy, MoITT, together with the Public Procurement Regulatory Authority (PPRA), Ministry of Finance, and other relevant authorities, shall devise mechanisms to move away from the conservative theme of Capital Expenditure to Operational Expenditure, which is more relevant for cloud service provisioning. Furthermore, guidance will be provided to PSE on the aforementioned aspects concerning procurement of cloud services.

10.1 Centralized Procurement

The true benefits of cloud computing can be realized with a centralized entity providing facilitation to PSE for their cloud procurement needs. This provides convenience, efficiency, reduced costs and a simplified ordering process. Aggregate demand for common cloud technologies by PSE results in the best possible offerings from CSP. It also aligns different PSE over a common set of terms and conditions rather than different ones for each organization. CAO will be the centralized office for ICT procurements of all PSE. CAO will have the visibility of the aggregate demand of PSE which will result in better cost and service offerings by CSP.

10.2 Contracts with CSP

The relevant Cloud Office will issue guidelines for the execution of cloud computing contracts between PSE and CSP. These guidelines will cover (but are not limited to) the following areas: -

10.2.1 Service Level Agreements (SLA)

SLA are undertakings that are binding on the CSP on the service level. Among other things, they stipulate penalties for the CSP if the contractual undertakings are not fulfilled. They are particularly important with regards to clauses on security (vulnerability scanning, patching and change management, quality control checks, certification requirements, etc) and data protection (retention period, exercise of rights of data subjects, availability of processing, etc.).

The provisioning of cloud solutions by CSP shall be governed by SLA by specifying and clarifying performance expectations and establishing accountability. The SLA shall relate to the provisions in the contract regarding incentives, penalties, escalation procedures, disaster recovery and business continuity, and contract cancellation for the protection of customers in the event the CSP fails to meet the required level of performance.

PSE shall closely monitor the CSP compliance with key SLA provisions among others on the following aspects:

a. Availability and timeliness of services;
b. Confidentiality and integrity of data;
c. Change control;
d. Security standards compliance, including vulnerability and penetration management;
e. Business continuity including disaster recovery and contingency plans; and
f. Help Desk Support.

10.2.2 Interoperability Requirements

PSE shall require interoperability of the components of cloud infrastructure to work together to achieve the intended result based on international standards. The components may come from different sources including public and private cloud implementations. The components shall be replaceable by new or different components from different CSP and continue to work, to facilitate the exchange of data between systems.

10.2.3 Migration between Cloud Service Providers

PSE may decide to change / migrate between CSP for a variety of reasons. Their initial migration to the cloud must facilitate future migration between platforms. This can be enabled by defining technology standards in their procurement processes. If PSE build their infrastructure using standard and widely available components, this will facilitate the migration of their data to the cloud and between CSP. PSE shall consider the necessity of migrating potentially large quantities of data to launch a service, and the ability to increase the scale if necessary. CAO will be available to facilitate in recommending models and roll out plans for PSE to follow for cloud adoption and migration between CSP.

10.2.4 Data Ownership

PSE will have full ownership of their data. They will decide how and where their data is stored and managed. Data kept on the cloud remains the property of the PSE irrespective of who owns, manages, or operates the cloud. PSE has the right to access, retrieve, modify or delete the data irrespective of the physical location of the cloud. It also has the right to approve, deny or revoke access to the data by third parties.

PSE shall consider how any data on the cloud can be retrieved and returned when the contract for cloud services expires. They shall ensure that the CSP specifies how data will be transferred back if required and agree on a timeline, which shall be included within the contract. Most importantly, all PSE shall instruct that the copies of the data will be deleted, overwritten, or otherwise rendered inaccessible upon expiration or termination of a contract. Moreover, CSP shall adhere to data protection regulations of GOP. CSP must not have the access or capability to monitor government data and content, maintaining strict adherence to the level of confidentiality, integrity and availability.

11 Date of Application and Validity

This policy becomes effective by the date it is provided approval by the competent authority. The policy is subject to holistic review as and when required

Annex-F: Minimum Suggested Requirements for Contracts

12 Annex A – Cloud Service Models

Cloud computing is available in three different service models. Each of these service models fulfils a unique set of business requirements. Following are the three service models of cloud computing.

12.1 Software as a Service (SaaS)

PSE can use the provider’s applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser. PSE does not manage or control the underlying cloud infrastructure. Examples of use include accounting, email, and document management tools.

12.2 Platform as a Service (PaaS)

The cloud infrastructure is PSE-created or PSE acquired applications created using programming languages and tools supported by the provider. The PSE does not manage or control the underlying cloud infrastructure including networking, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Examples include databases, programming environments, and video teleconferencing tools.

12.3 Infrastructure as a Service (IaaS)

PSE can provision processing, storage, networks, and other fundamental computing resources where the PSE can deploy and run arbitrary software, which can include operating systems and applications. PSE does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (such as host firewalls). Examples include networking storage and virtualisation servers.

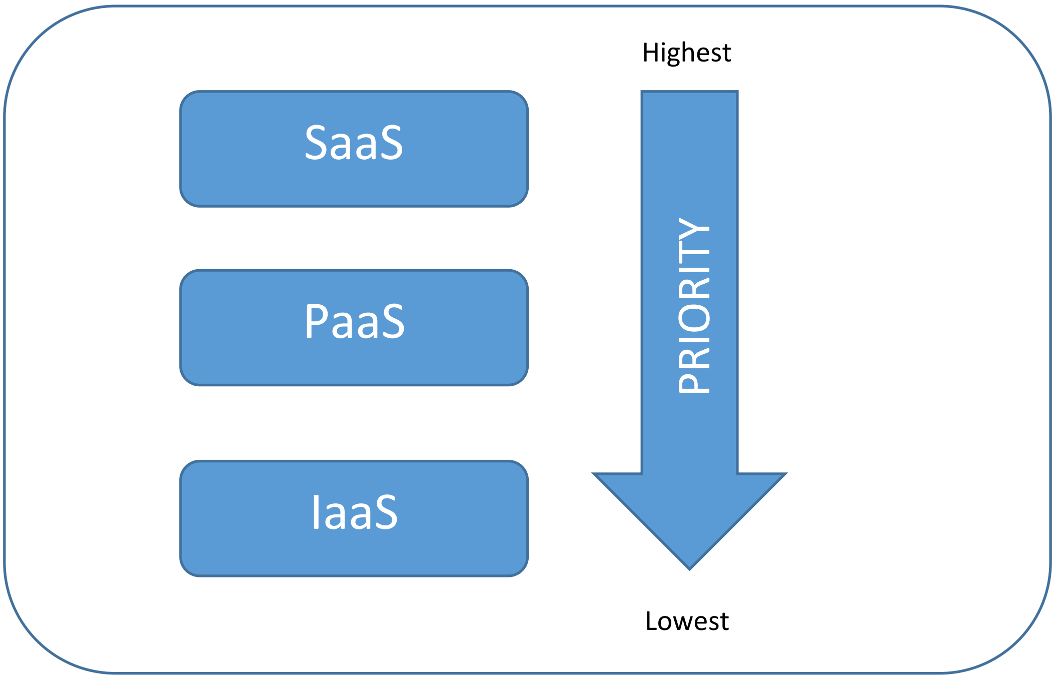
13 Annex B – Priority of Cloud Service Models

PSE may consider the following priority in terms of the cloud service model. However, the selection of a particular type of cloud model is dependent on the requirements of the PSE.

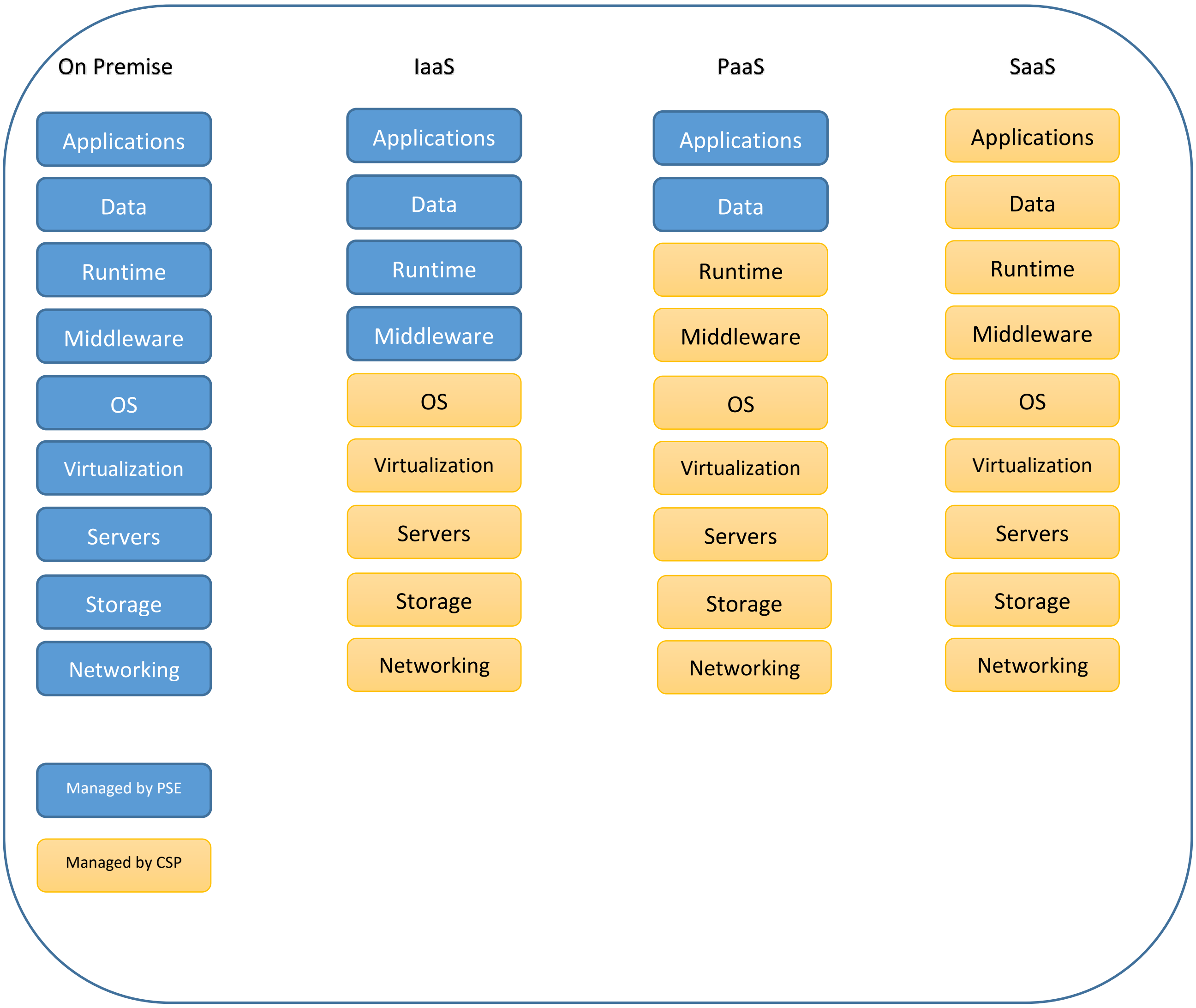
1- Software as a Service (SaaS)
This type of service model is the preferred model. It maximizes the benefits offered by the cloud.

2- Platform as a Service (PaaS)
This type of service model is preferred when SaaS is not available or is not feasible.

3- Infrastructure as a Service (IaaS)
This type of service model is preferred when SaaS and PaaS are not available or are not feasible



14 Annex C – Share of Responsibilities between CSP and PSE



On Premise	IaaS	PaaS	SaaS
🟦 Applications	🟦 Applications	🟦 Applications	🟨 Applications
🟦 Data	🟦 Data	🟦 Data	🟨 Data
🟦 Runtime	🟦 Runtime	🟨 Runtime	🟨 Runtime
🟦 Middleware	🟦 Middleware	🟨 Middleware	🟨 Middleware
🟦 OS	🟨 OS	🟨 OS	🟨 OS
🟦 Virtualization	🟨 Virtualization	🟨 Virtualization	🟨 Virtualization
🟦 Servers	🟨 Servers	🟨 Servers	🟨 Servers
🟦 Storage	🟨 Storage	🟨 Storage	🟨 Storage
🟦 Networking	🟨 Networking	🟨 Networking	🟨 Networking

🟦 Managed by PSE

🟨 Managed by CSP

15 Annex D – Data Classification Guidelines

This policy lists the following five simple classes of data. Data classification standards are governed by appropriate data classification guidelines of the Government of Pakistan.

a. Open Data

Publicly available data structured in a way that the data is fully discoverable and usable by end users is called ‘open data’. The implementation of open data principles in the public sector makes the government open and accountable and increases citizen participation in government. The PSE classifying any data as Open Data must share the criteria with Cloud Office.

b. Public data

Data related to the public sector that is non-confidential and is publicly available.

c. Restricted data

Data related to public sector business, operations, and services which even if publicly available but a compromise of which can undermine the reputation of Pakistan internationally.

d. Sensitive/Confidential data

Information not intended to be published, which shall be accessed only by certain people having proper authorization and which justifies moderate protective measures.

- Phone numbers, registration numbers (BVN, vehicle, etc.), passport, etc.
- Information that contains at least one personally identifiable information (PII) like name (first and last), address, biometrics, etc.
- Data classified as “confidential” and, perhaps, certain categories of “secret” data (e.g. Obsolete or archived “secret” information).
- Information accessible through Intranet only, but available to broadly defined categories of authorized officials and public servants. Drafts of laws and regulations that are not yet in the public domain.

e. Secret

Secret information requiring the highest level of protection from serious threats, whose breach will likely cause threats to life or public security, financial losses, serious damage to public interests, etc.

- Lead directly to widespread loss of life.
- Threaten directly the internal stability of Pakistan or friendly nations.
- Raise international tension.
- Cause exceptionally grave damage to relations with friendly nations.
- Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.
- Cause long -term damage to the Pakistani economy.
- Cause major, long-term impairment to the ability to investigate or prosecute serious organised crime.

16 Annex E – Cloud Selection Matrix for Government Data

Public Sector Data Classification	Type of Cloud	Security in Place
Open Data	Public Cloud by Registered CSP	Baseline
Public	Public Cloud by Accredited CSP	Baseline
Restricted	Government Cloud by Accredited CSP	Intermediate
Sensitive/Confidential	Government Cloud by Accredited CSP	Enhanced
Secret	Private (Cloud in use by a single organization) or Government Cloud by Accredited CSP	Highest

Further details of what constitute baseline, intermediate, enhanced and highest will be laid out by the Cloud Office in line with domestic and international benchmarks.

17 Annex F – Minimum Suggested Requirements for Contracts

a. CSP's adherence to the due diligence process and conformity of public procurement guidelines/processes;

b. a clear description of services to be provided;

c. the contract's duration (unless it is of unlimited duration);

d. payment terms and termination and dispute settlement mechanism;

e. details on the available Service Level Agreements (SLAs);

f. rules on handling cloud customer data, including their processing, destruction, and restoration;

g. CSP's customer care services depending on a particular service offering;

h. customers' right to retrieve their data stored in the CSP's system, if the cloud contract is terminated; and

i. limitation of CSPs' right to exclude their liability unreasonably or to impose unfair contract terms related, for instance, to any loss of, or damage to, customer's data, quality of service degradations such as service unavailability, or data breaches. NOTE: a bit clustered