Republic of the Philippines
Office of the Solicitor General
134 Amorsolo St. Legaspi Village, Makati City

Technical Working Group for ICT-Subscription

TERMS OF REFERENCE

Subscription of Cloud Computing Platform for OSG

Background:

Cloud computing has revolutionized how organizations manage and utilize technology resources. It offers scalability, flexibility, and cost-effectiveness by providing Internet access to a pool of computing resources. A subscription-based model allows organizations to pay for the resources they use, promoting efficiency and agility in their operations.

The Office of the Solicitor General intends to leverage cloud computing, aligning with the Government's "Cloud First Policy." [1]This shift aims to enable seamless, immediate access to a configurable pool of computing resources, including networks, servers, storage, applications, and services, adhering to the mandate to modernize its server and backup infrastructure partially.

This strategic migration to the cloud will aid the agency in curtailing ICT acquisition and operation costs, fostering operational excellence, bridging security gaps, enhancing employee productivity, and facilitating the development of robust online services.

Objective:

The OSG's primary objective is to provide the organization with a predictable cost structure while enabling the flexibility to scale resources as needed. With 'top-up' functionality, the OSG can increase its commitment balances at any time, ensuring uninterrupted access to resources and accommodating sudden spikes in demand without disrupting operations. The OSG aims to optimize cost-efficiency while adapting to evolving organizations' requirements in the digital landscape.

The subscription to cloud computing services will maintain the performance and functionality of its systems and ensure its compatibility with the existing setup of OSG application systems and databases.

[1] DICT Department Circular (DC) No. 010 Series of 2020 Amending DC 2017-002 re: Prescribing the Philippine Government's Cloud First Policy, which states that all government agencies shall adopt cloud computing as the preferred ICT deployment strategy for the delivery of government services.

Terms:

1. *Scope.* – **Subscription of Cloud Computing Platform for OSG**

2. *ABC.* - The Approved Budget for the Contract (ABC) is **Five Million Five Hundred Thousand Pesos only (PHP 5,500,000.00) for twelve (12) months,** inclusive of all government taxes, charges, and other standard fees.

ICT SUBSCRIPTION			
ITEM	**QTY**	**UNIT COST**	**TOTAL**
Subscription of Cloud Computing Platform for OSG	**1**	5,500,000.00	5,500,000.00
		TOTAL	**₱ 5,500,000.00**

3. *Subscription Duration* - 12 months subscription as an upfront monetary commitment, with usage-based consumption. "Top-up" enabled for additional commitment balances anytime if required.

4. *Schedule of Payment.* - To guarantee the performance by the winning bidder of its obligations under the contract, it shall post a performance security before the signing of the contract. The performance security shall be in an amount not less than the required percentage of the total contract price in any of the following forms and in accordance with the following schedule:

Form of Performance Security	Amount of Performance Security (Not less than the required % of the Total Contract Price)	Statement of Compliance
a) Cash or cashier's/ manager's check issued by a Universal of Commercial Bank.	5%	
b) Bank draft/ guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank; *however,* it shall be confirmed or authenticated by a Universal or Commercial Bank if issued by a foreign bank.	5%	
c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	30%	

TERMS OF PAYMENT	Statement of Compliance
Supplier agrees to be paid based on the billing scheme as follows:	
• Within thirty (30) days from completion of the delivery and issuance of the Inspection and Acceptance Report by the OSG and submission of all other required documents - 95% of the contract price. • One (1) year from the issuance of the Inspection and Acceptance Report by the OSG - 5% of the contract price.	

All bid prices shall be considered as fixed prices and, therefore, not subject to price escalation during contract implementation.

5. *Qualifications of the Supplier*:

a) The bidder must have completed, within the last three years from the submission date and receipt of at least one (1) single contract of a similar nature amounting to at least twenty-five percent (25%) of the ABC. The definition of a similar contract is the provision of a cloud platform.

b) The service provider must have proof of the necessary eligibility, experience, and expertise in providing the service, with the following credentials:

1. The prospective service provider must be at least three (3) years as an authorized distributor of the cloud computing platform, as attested through a signed manufacturer's certification. A signed local distributor's certification is needed when a reseller, partner, or dealer is involved.
2. The Supplier must have satisfactorily completed at least (3) projects similar to the proposed cloud solution.
3. The prospective service provider must have Cloud Platform Certified Engineers employed locally with a certification from the Cloud Provider (offered). A

certificate of employment and a transcript are also required. Below is the list of ALL required engineers.

- Must have at least one (1) Cloud Solutions Architect Expert
- Must have at least one (1) Cloud Administrator Associate
- Must have at least one (1) Cloud Security Certified Engineer.

6. *Delivery*

a) The subscription shall be provided to OSG within ten (10) days upon receipt of NTP and must be before the anniversary date of its existing cloud platform (May 31, 2025).

b) The service provider shall demonstrate that the requirements specified by OSG are properly provisioned and configured, including all the necessary migration and customization.

7. *Warranty/ Product Support Requirement*

The Service provider should provide a notarized undertaking that it will provide the warranty/after-sale support requirement, as follows:

a) Provide one (1) year of standard support services.

b) For technical assistance, the contact person would be designated by the subscription provider and support through email/online/phone for the entire subscription duration with complete end-to-end customer management such as value-added services, provisioning, management, billing, and technical support from the service provider. The contact person may be required to visit OSG if deemed necessary.

c) The winning bidder must provide eight (8) hours x five (5) days of technical support through unlimited phone, email, remote, and chat.

d) Must have a high priority level for the Cloud Provider Technical Support available eight (8) hours x five (5) days with unlimited phone, email, remote, and chat assistance.

e) The winning bidder will provide technical support covering the following but not limited to:

- Online incident submission
- Less than 4 hours response time upon receipt of the request from OSG.
- Consulting services on related support and services,

f) Furnish OSG the monthly data usage/consumption report.

8. *Knowledge Transfer*

a) The Supplier shall provide Administration training for the proposed cloud solution for 12 participants.

b) The training shall be conducted face-to-face, led by a Certified Engineer/Trainer. If a Certified Engineer/Trainer is unavailable locally, online/virtual training shall be allowed, provided learning tools and materials shall be accessible/provided to the participants.

c) The knowledge transfer and training for end users (IT) should be within the 10-day delivery period.

9. Applicable provisions of the Government Procurement Reform Act (RA No. 9184) and its Revised Implementing Rules and Regulations (RIRR) shall form part of the Terms of Reference.

==========================

Technical Specifications:

ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING PLATFORM	Statement of Compliance
On-demand Self-service. Unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with CSP.	
Broad Network Access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).	
Resource Pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the agency's demand. There is a sense of location independence since the government agency generally has no control or knowledge over the exact location of the provided resources but may be able to specify the location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.	
Rapid Elasticity. Capabilities can be elastically provisioned and released, in some cases, automatically, to scale rapidly outward and inward commensurate with demand. To the end-user, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.	
Measured Service. Cloud systems automatically control and optimize resource use 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.	
SECURITY	
The CSPs should meet international security standards and should abide by all relevant Philippine laws and industry standards.	
Data that can be migrated to the public cloud will need to meet security requirements for accreditation and be verified by internationally recognized security assurance frameworks. Accepted international security assurance controls include ISO/IEC 27001 and 27018, Service Organization Controls Report (SOC) 1 and 2, and the Payment Card Industry Data Security Standard (PCI DSS).	

Data will be encrypted using industry-tested and accepted standards and algorithms, such as AES (128 bits and higher	

Service Features	Requirements	Compliance
Availability	The online subscription to the cloud computing platform shall be made available 24/7 to the authorized users of the OSG throughout the entire duration of the 1-yr subscription.	
SCOPE OF SERVICES		
The web hosting service and standard web hosting support service provider shall: • Supply and deliver the required services stipulated in the Purchase Request • The cloud service provider, through its local counterpart technical support, will be responsible for provisioning the required cloud platform, services, and associated licenses with the following specifications to ensure compatibility with OSG continuous services:		
Traffic Management	Capability to control the distribution of traffic across application endpoint. Continuous monitoring of endpoint health and status	
IP Requirement	Provide public IP resources to communicate with other cloud resources, on-premises networks, and the internet	
Security	Inclusion of a unified security management platform that includes security health monitoring of cloud workloads, and security threat blocking through access and application control	
Privacy	Must adhere to the Data Privacy Act of 2012 (RA 10173), must offer continuous security health monitoring for the entire cloud environment	
Scalable Resources	Provide the capability to increase/decrease resources as needed to support any periods of unpredictable resource usage. Scalable resources must include Bandwidth,	

	Servers, Storage, and Database instances	
Vendor Support	Virtual machine availability and connectivity must be at least 99% up all the time	

MINIMUM REQUIRED SPECIFICATIONS / FEATURES

DESCRIPTION	Statement of Compliance
GENERAL REQUIREMENTS	
1. Hosting the cloud-based systems developed and implemented by the OSG.	
2. Fully compatible and integrated with the existing cloud-hosting platform of OSG.	
3. Fully compatible to integrate with OSG's existing on-premises environment.	
4. First-party single sign-on capability with OSG's identity and access management service	
5. The proposed cloud solution must be in the "leader's quadrant" in the Cloud Infrastructure and Platform Services in the Gartner Magic Quadrant of 2023.	
6. The solution must be in an Infrastructure-as-a-Service environment and Platform-as-a-Service Environment	
7. Continuously use the existing OSG tenant account	
8. The solution must support Platform as a Service – it provides a platform allowing one to develop, run, and manage applications without the complexity of building and maintaining the infrastructure.	
9. The solution should enable seamless resource/workload movement from cloud source to destination.	
10. The cloud service provider offers better security for applications and data than the security would attain in-house.	
11. The solution must have an IaaS that provides all the infrastructure to support web apps, including storage, web and application servers, and networking resources.	

12. The solution must have a framework for easily building and customizing cloud-based applications	
13. The solution must support geographically distributed development teams	
14. The solution must efficiently manage the application lifecycle	
15. The solution must have an IaaS that makes it quick and economical to scale dev/test environments up and down.	
16. The solution must simplify the planning and management of backup and recovery systems.	
17. The solution must have a Web Application Firewall (WAF).	
18. The solution must have a Managed DNS.	
19. The solution must have a Managed SQL database in the cloud.	
20. The solution must have a Cloud-native application protection platform (CNAPP).	
21. All data at rest and in transit must be encrypted.	
22. The solution must have a DevOps tool	
23. The solution must have equivalent server specifications based on the existing solution.	
24. The solution must retain the current fully qualified domain name	
25. The solution must be capable and compatible with hosting the existing cloud environment	
26. The cloud SQL database must be accessible anywhere to update the table contents but must have proper security measures.	
27. The solution must have an interactive Graphical User Interface (GUI) accessible in any location, allowing the cloud administrators and development teams to conveniently access, manage, provision, and modify all cloud services and components instantly and securely. Multi-factor Authentication is recommended.	

28. The solution must have monitoring tool/s for application performance, analytics, system health, and diagnostic logs.	
29. The winning bidder must provide As-Built documentation or manual, including testing results.	
30. The winning bidder will be responsible for migrating instances and workloads from MS Azure to another provider if the present platform or provider differs from the hosted solution.	
SECURITY REQUIREMENTS	
1. Security has the feature of continually assessing the security posture, tracking new security opportunities, and precisely reporting progress.	
2. Security can secure the workloads with step-by-step actions that protect the workloads from known security risks.	
3. Security can generate a secure score for your subscriptions based on an assessment of your connected resources	
4. Security can detect threats targeting Cloud services, including Web App Services, SQL, Cloud Storage Accounts, and more data services.	
5. security can defend the workloads in real-time so can react immediately and prevent security events from developing.	
6. The security has advanced threat protection features for virtual machines, SQL databases, containers, web applications, your network, and more	
7. security can help limit exposure to brute force attacks.	
8. The security has capabilities that help automatically classify data in SQL.	
WEB APPLICATION FIREWALL	
1. Must have protection against web vulnerabilities and attacks.	
2. Must be capable of protecting multiple websites or applications.	

3. WAF Policies must be customizable for each web application.	
4. Protection against malicious bots and IPs.	
5. Must have protection against common attacks such as SQL Injection, cross-site scripting, command injection, HTTP hi-jacking, HTTP protocol violation and anomalies, crawlers, and scanners.	
6. Must have geo-location filtering.	
7. Must be capable of inspecting JSON and XML.	
8. Must be integrated and configured with the centralized monitoring tool for centralized monitoring.	
9. Must have customizable rules/policies to suit application requirements	
10. Must have logging and monitoring that can be saved or imported to PDF for printing.	
11. Must be integrated and configured with the centralized monitoring tool.	
INFRASTRUCTURE	
1. Must have a financially backed service level agreement (SLA) that guarantees monthly availability.	
2. Must provide preferential discounts for Virtual Machine services for securing longer term consumption and Bring Your Own License (BYOL) with corresponding software maintenance program.	
3. Must provide extended security updates for Windows Server 2012 and SQL Server 2012 workloads moving to the cloud without additional cost.	
4. Must provide additional 3-year extended security updates for Windows Server 2012 and SQL Server 2012 workloads moving to the cloud with additional cost.	

==========================

BILL OF MATERIALS

Service category	Service type	Region	Description
Networking	Application Gateway	Southeast Asia	Web Application Firewall V2 tier, 734 Fixed gateway Hours, 1 compute unit and 1,000 persistent connections with 1 mb/s throughput, 5 GB Data transfer
Compute	App Service	Southeast Asia	Free Tier; 1 F1 (0 Core(s), 1 GB RAM, 1 GB Storage) x 730 Hours; Linux OS
Compute	App Service	Southeast Asia	Premium V2 Tier; 2 P1V2 (1 Core(s), 3.5 GB RAM, 250 GB Storage) x 730 Hours; Linux OS; 0 SNI SSL Connections; 0 IP SSL Connections; 0 Custom Domains; 0 Standard SLL Certificates; 0 Wildcard SSL Certificates
Compute	App Service	Southeast Asia	Standard Tier; 2 S1 (1 Core(s), 1.75 GB RAM, 50 GB Storage) x 730 Hours; Linux OS; 0 SNI SSL Connections; 0 IP SSL Connections; 0 Custom Domains; 0 Standard SLL Certificates; 0 Wildcard SSL Certificates
Databases	Azure Database for MySQL	Southeast Asia	Flexible Server Deployment, Burstable Tier, 2 B1MS (1 vCores) x 730 Hours, 20 GB Storage with LRS redundancy, 0 million Paid IO, 0 GB Additional Backup storage with LRS

Databases	Azure Database for MySQL	Southeast Asia	Single Server Deployment, General Purpose Tier, 2 Gen 5 (2 vCore) x 730 Hours, 50 GB Storage with ZRS redundancy, 0 GB Additional Backup storage - LRS redundancy
Networking	Azure DNS		Zone 1, DNS, Private; 2 hosted DNS zones, 0 DNS queries
Networking	Azure Front Door		Azure Front Door Standard - Base instance included, 5 GB Data Transfer Out to Client, 5 GB Data Transfer In to Origin, 0 x 10,0000 Requests
Developer tools	Azure DevOps		7 Basic Plan license additional users, 0 Basic + Test Plans license users, Free tier - 1 Microsoft Hosted Pipeline(s), 1 Self Hosted Pipeline(s), 0 GB Artifacts, 0 GitHub Advanced Security committers
Management and governance	Azure Backup	Southeast Asia	Azure VMs, Standard Backup policy, 5 Instance(s) x 1 GB, GRS Redundancy, Moderate Average Daily Churn, 9,728 GB Average monthly backup data in Standard Tier, 0 GB Average monthly backup data in Archive Tier
Networking	Bandwidth		Inter Region transfer type, 1000 GB outbound data transfer from Southeast Asia to East Asia

Storage	Storage Accounts	Southeast Asia	Block Blob Storage, Blob Storage, Flat Namespace, LRS Redundancy, Cool Access Tier, 1,000 GB Capacity - Pay as you go, 1,000 x 10,000 Write operations, 1,000 x 10,000 List and Create Container Operations, 1,000 x 10,000 Read operations, 1,000 x 10,000 Other operations. 100 GB Data Retrieval, 1,000 GB Data Write, SFTP disabled
Networking	IP Addresses	Southeast Asia	Standard (ARM), 1 Static IP Addresses X 730 Hours, 0 Public IP Prefixes X 730 Hours
Security	Key Vault	Southeast Asia	Vault: 533 operations, 0 advanced operations, 0 renewals, 0 protected keys, 0 advanced protected keys; Managed HSM Pools: 0 Standard B1 HSM Pool(s) x 730 Hours
Security	Microsoft Defender for Cloud	Southeast Asia	Microsoft Defender for Cloud Workload Protection: 0 Plan 1 servers x 730 Hours, 2 Plan 2 servers x 730 Hours, 0 Container vCores x 730 Hours, 0 additional container image scans, 8 App Service nodes x 730 Hours, 0 SQL Database servers on Azure, 0 SQL Database servers outside Azure x 730 Hours, 4 MySQL Instances, 0 PostgreSQL Instances, 0 MariaDB Instances x 730 Hours, Cosmos DB 0 x100 RU/s x 730 Hours, 80 Storage accounts x

			730 Hours with 0 million total overage of transactions across each storage account and 0 GB storage scanned for malware, Defender for APIs - Plan 1 with 0 estimated API monthly transactions, 760 Key Vault(s), 0 Subscription(s)
Networking	Bandwidth		Internet egress, 2000 GB outbound data transfer from Southeast Asia routed via Microsoft Global Network
Storage	Storage Accounts	Southeast Asia	Managed Disks, Standard HDD, S10 Disk Type 2 Disks, 100 Storage transactions
Storage	Storage Accounts	Southeast Asia	Managed Disks, Standard HDD, S30 Disk Type 25 Disks, 100 Storage transactions
Storage	Storage Accounts	Southeast Asia	Page blobs (Unmanaged Disks included), Standard, LRS Redundancy, General Purpose V2, 100 GB Capacity, 100 Operations for Unmanaged Disks, 4 Write operations for Page Blobs, 0 Write additional IO units, 9 Read operations for Page Blobs, 0 Read additional IO units, 10,000 Delete operations for Page Blobs
Storage	Storage Accounts	Southeast Asia	Table Storage, Standard, LRS Redundancy, 100 GB Capacity, 2.99 Storage transactions

==========================

Storage	Storage Accounts	Southeast Asia	Block Blob Storage, Blob Storage, Flat Namespace, LRS Redundancy, Archive Access Tier, 1,000 GB Capacity - Pay as you go, 0 x 10,000 Write operations, 0 x 10,000 List and Create Container Operations, 0 x 10,000 Read operations, 100,000 Archive High Priority Read, 1 x 10,000 Other operations. 1,000 GB Data Retrieval, 1,000 GB Archive High Priority Retrieval, 1,000 GB Data Write, SFTP disabled
Storage	Storage Accounts	Southeast Asia	Block Blob Storage, General Purpose V2, Flat Namespace, LRS Redundancy, Hot Access Tier, 100 GB Capacity - Pay as you go, 15 x 10,000 Write operations, 14 x 10,000 List and Create Container Operations, 0 x 10,000 Read operations, 0 x 10,000 Other operations. 1,000 GB Data Retrieval, 1,000 GB Data Write, SFTP disabled
Compute	Virtual Machines	Southeast Asia	3 A4 v2 (4 Cores, 8 GB RAM) x 730 Hours (Pay as you go), Windows (License included), OS Only; 1 managed disk – E10; Inter Region transfer type, 5 GB outbound data transfer from Southeast Asia to East Asia
Networking	Virtual Network		Southeast Asia (Virtual Network 1): 100 GB Outbound Data

			Transfer; Southeast Asia (Virtual Network 2): 100 GB Outbound Data Transfer
Networking	VPN Gateway	Southeast Asia	VPN Gateways, VpnGw1 tier, 730 gateway hour(s), 0 additional S2S tunnels (beyond included amount), 0 additional P2S connections (beyond included amount), 0 GB, Inter-VNET VPN gateway type
DevOps	Azure Monitor	Southeast Asia	Log analytics: Log Data Ingestion: 8 GB Daily Analytics logs ingested, 0 GB Daily Basic logs ingested, 10 months of Interactive Data Retention, 0 months of data archived, 0 GB data restored for 0 days, 0 Basic Log Search Queries per day with 0 GB data scanned per query, 0 GB of Log Data Exported per day, Platform Log Data Processed per day: 0 GB with Destination to Storage or Event Hub and 0 GB with Destination to Marketplace Partners, 0 Search job Queries per day with 0 GB data scanned per query; 0 SCOM MI Endpoints; Managed Prometheus: 0 AKS nodes in cluster, 10000 Prometheus metrics per node, 30 seconds of Metric collection interval, 0 Average daily Dashboards users, 7 Dashboards, 50000 Data

			samples queried per dashboard, 25 promql alerting rules, 25 promql recording rules; Application Insights: 3 months Data retention, 0 Standard Web Tests, 5 Minutes Execution frequency, Executing for 730 hours; 0 resources monitored X 1 metric time-series monitored per resource, 5 Minutes Log Signal frequency with 0 log signals monitored and {2} time series per signal, 0 Additional events (in thousands), 0 Additional emails (in 100 thousands), 0 Additional push notifications (in 100 thousands), 0 Additional web hooks (in millions)
Networking	Azure Bastion	Southeast Asia	Standard Tier, 730 Hours, 0 Additional Scale Units, 5 GB Outbound Data Transfer
Support		**Support**	

==========================

Technical Working Group for ICT Subscriptions

SSS JOEL N. VILLASERAN

DIR IV EDUARDO ALEJANDRO O. SANTOS

ITO III JAYVIE NEIL MALICK S. MALICDEM

ITO II CEDRIC S. DELA CRUZ

SAO JOY Y. CHUA

CMT III JESUS NIÑO CHUA

AO IV RAY CHARLIE V. ALEGRE

Approved/Disapproved:

MENARDO I. GUEVARRA
Solicitor General

Certified Funds Available:

BERNADETTE M. LIM
Dir IV - FMS