



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF TRANSPORTATION
MARITIME INDUSTRY AUTHORITY

TECHNICAL SPECIFICATIONS

Project Description	SUBSCRIPTION OF CLOUD BASED HOSTING FOR MARINA BLOCKCHAIN ENABLED CERTIFICATION SYSTEM (MBEST)
Rationale and Brief Background	<p>Cloud hosting provides a modern, efficient, and fit-for-purpose solution for the management and delivery of government digital systems and services. Its inherent scalability, cost efficiency, high availability, performance optimization, security, and accessibility support the Government's objectives of ensuring reliable public service delivery while optimizing the use of public funds. Through cloud infrastructure, computing resources may be scaled based on actual demand, allowing agencies to pay only for resources utilized, thereby minimizing idle capacity and unnecessary capital expenditures. High uptime guarantees, automated maintenance, and continuous technical support further contribute to operational efficiency and service continuity.</p> <p>Consistent with the principles of Republic Act No. 12009 (New Government Procurement Act)—particularly value for money, efficiency, economy, sustainability, and lifecycle cost management—cloud computing enables government agencies to adopt technology solutions that are resilient, secure, and adaptable to evolving operational requirements. Cloud platforms also support enhanced data protection through advanced security controls and enable authorized access to systems and information anytime and anywhere via secure internet connectivity, in line with government digitalization and interoperability initiatives.</p> <p>In support of these objectives, the Maritime Industry Authority (MARINA) recognizes the need to ensure uninterrupted, reliable, and secure operation of its digital services, particularly those critical to maritime certification and regulatory functions. The MARINA Blockchain Certification System (MARINA-BEST) was previously deployed and hosted by the Department of Information and Communications Technology (DICT) using the Google Cloud Platform (GCP). To maintain operational stability, system integrity, and continuity of service, MARINA shall procure a</p>

	<p>fit-for purpose cloud computing platform that will effectively and efficiently support the MARINA-BEST system.</p> <p>This approach ensures the sustained reliability, security, and availability of the system while avoiding service disruption, duplication of resources, and additional transition risks. It is consistent with the Agency's digital transformation agenda and the procurement policy direction under RA 12009, which encourages the adoption of efficient, secure, scalable, and sustainable solutions that deliver measurable value and uninterrupted public service.</p>
<p>Objective</p>	<p>The primary objective of this initiative is to ensure the continuity, reliability, and security of the MARINA Blockchain Certification System (MARINA-BEST) through the continued use of a cloud computing environment that meets the system's operational, security, and scalability requirements currently supporting the MARINA-BEST system.</p> <p>Specifically, the initiative seeks to:</p> <ol style="list-style-type: none"> 1. Sustain uninterrupted service delivery and operational stability of the MARINA-BEST system to effectively support the Agency's digital certification processes; 2. Utilize cloud platform features comparable to the existing infrastructure, including scalability, high availability, and robust security controls, to improve system performance and ensure data integrity and protection; 3. Advance MARINA's digital transformation objectives through the adoption of secure, scalable, and sustainable cloud-based infrastructure that supports efficient deployment and management of online services; 4. Promote cost-efficient and optimized resource utilization through usage-based consumption models and automated system management capabilities; and 5. Enhance service accessibility and responsiveness by enabling secure, reliable access to system resources anytime and anywhere through internet connectivity.
<p>Approved Budget of the Contract</p>	<p>The Approved Budget for the Contract (ABC) amounts to Twenty-Five Million Pesos and 00/100 (PHP 25,000,000.00), inclusive of VAT and other applicable government taxes to be charged against the General Appropriations Act (GAA) FY 2026.</p>
<p>Specifications/Deliverables</p>	<ol style="list-style-type: none"> 1. Scalable Cloud Hosting for MARINA core systems. The Cloud Hosting for MARINA core systems will encompass both production and test environments.

	1.1 The hosting coverage is for one year and includes cloud services such as Compute, Storage, Networking, Identity and Security, Management Tools, Developer Tools, Monitoring Tools, Databases, and APIs.
--	---

**TECHNICAL REQUIREMENTS
(Infrastructure Breakdown Aligned with RA 12009)**

I. GENERAL REQUIREMENTS

1. The solution shall be deployed on a cloud-based infrastructure that ensures high availability, scalability, and security, and shall continue to utilize a cloud computing environment that meets the operational, security, and scalability requirements necessary to support the existing MARINA-BEST system setup.
2. All infrastructure components shall meet the **minimum specifications** stated herein; bidders may offer higher specifications at no additional cost but must align and support to the existing MARINA-BEST system setup.
3. Auto-scaling capabilities shall be enabled to ensure system performance during peak usage.
4. Infrastructure must support **production, staging, and training environments**.
5. The system shall comply with applicable **Philippine government ICT standards**, data privacy requirements, and cybersecurity best practices.

II. MODULE-SPECIFIC INFRASTRUCTURE REQUIREMENTS

A. SEAFARER MODULE

Cloud Service	Instance Name	Specification
Virtual Machine Service	marina-seafarer-vm-bastion	micro (2 vCPU, 1 GB RAM, 20 GB Disk)
Virtual Machine Service	marina-seafarer-vm-blockchain	16 vCPU, 32 GB RAM, 500 GB SSD Disk)
Managed Relational Database Service	marina-seafarer-mysql	24 vCPU, 64 GB RAM, 1,000 GB SSD

Cloud Service	Instance Name	Specification
Managed Server	marina-seafarer-backend	Auto-scale: 2–20 replicas, 16 vCPU, 32 GB RAM
Managed Server	marina-indexer-seafarer	Auto-scale: 2–12 replicas, 16 vCPU, 32 GB RAM
Managed Server	marina-seafarer-frontend	Auto-scale: 1–5 replicas, 16 vCPU, 32 GB RAM
Managed Server	marina-seafarer-admin	Auto-scale: 1–5 replicas, 16 vCPU, 32 GB RAM
Storage	marina-seafarer	
	mismo-dump	

B. SHIPPING MODULE

Cloud Service	Instance Name	Specification
Virtual Machine Service	marina-shipping-vm-bastion	micro (2 vCPU, 1 GB RAM, 20 GB Disk)
Virtual Machine Service	marina-shipping-vm-blockchain	8 vCPUs (vCPU) ,32 GB RAM, 500 GB SSD Storage
Managed Relational Database Service	marina-shipping-mysql	8 vCPU, 32 GB RAM, 1,000 GB SSD
Managed Server	marina-shipping-backend	Auto-scale: 2–20 replicas, 16 vCPU, 32 GB RAM
Managed Server	marina-shipping-frontend	Auto-scale: 1–5 replicas, 16 vCPU, 32 GB RAM
Managed Server	marina-shipping-admin	Auto-scale: 1–5 replicas, 16 vCPU, 32 GB RAM

Cloud Service	Instance Name	Specification
Storage	marina-shipping	
	samis-dump	
	oss-dump	

OS

Component	Specification
OS	Debian / Ubuntu / CentOS / CoreOS / BYOL

Region

Component	Specification
Region	Southeast Asia–based data center region or equivalent

III. SECURITY AND ACCESS REQUIREMENTS

1. A **Bastion Host** shall be used for controlled administrative access.
2. Role-based access control (RBAC) shall be implemented for all modules.
3. Database and storage shall have **encryption at rest and in transit**.
4. Audit logs shall be enabled for system and database activities.

IV. AVAILABILITY AND PERFORMANCE REQUIREMENTS

1. Production databases shall be configured with **High Availability (HA)**.
2. Auto-scaling thresholds shall ensure uninterrupted service during peak demand.
3. System shall support concurrent access across all modules without performance degradation.

2. Cloud hosting services must assist in the configuration / installation / migration from on-prem and setup of the MARINA Blockchain Enabled Certification Systems.
3. Cloud hosting services must have an auto-scaling feature.
4. Cloud hosting services must allow the creation of customized VMs where CPU and Memory can be set independent of each other.
5. Cloud hosting provider must encrypt data at rest and in transit by default.
6. Cloud hosting services must support the use of open-source server operating systems, open-source web servers, and open-source databases.

7. Cloud hosting services must be capable of supporting online access to web applications from users located anywhere in the world and must not have geographical limitations.
8. Cloud hosting service must have a user-accessible dashboard and portal for metrics and to allow for modifications to allocated server resources.
9. Cloud hosting services must keep logs of network traffic, usage, and connection metrics.
10. Cloud hosting services must be secure and provide features for building secure application workloads.
11. Provision for a Web Application Firewall or WAF, whether as part of the hosting service itself or from a reputable third-party.
12. The proposed solution shall provide an in-country cloud infrastructure hosted within the Philippines to ensure compliance with the Philippine Government Cloud First Policy, Data Privacy Act (RA 10173), and related data sovereignty regulations. The solution must implement redundancy and backup within Philippine territory to ensure data availability, disaster recovery, and jurisdictional control. The cloud infrastructure shall be hosted in a data center located in the Philippines and certified to Tier III standards by a recognized third-party certification body (e.g., Uptime Institute) or an equivalent international standard demonstrating concurrent maintainability and high availability. The bidder shall submit valid proof of certification and compliance during post-qualification.
13. Includes technical administration and support services to manage cloud-hosting service and WAF configuration with the allocation of the following remote personnel:
 - 13.1 Professional Cloud Architect Two (2) - responsible for conversion of MARINA requirements into a custom-fit cloud architecture and design and is primarily accountable for code, execution and quality reviews of the cloud solution.
 - 13.2 Professional Cloud Developer Three (3) - responsible for management of cloud environments and implementation of instances required by MARINA platforms.
 - 13.3 Professional Data Engineer One (1) - responsible for the review and management of the data pipeline and processing efficiency of the instances maintained by MARINA platforms.
 - 13.4 Professional Cloud Security Engineer One (1) - responsible for ensuring the security of the Web Application Firewall and other cloud configurations of the instances maintained by MARINA platforms.
14. Includes Managed Services from the service provider for one (1) year.

14.1 Managed Services includes the setup and documentation of Cloud Organization.

14.2 Managed Services includes provisioning and configuration of new cloud resources.

14.3 Managed Services includes the modification of cloud infrastructure with the intent to improve stability, reliability, scalability, performance, and availability, or reduce the cost of the agency's cloud environment.

14.4 Managed Service and Support exclude:

14.4.1 Application development and testing.

14.4.2 Any activity that requires the handling of application or user data.

14.4.3 Any activity that includes the modification of application code.

15. Includes Technical Platform Support from the service provider for one (1) year.

15.1 Technical Platform Support includes platform support for MARINA application development teams on a request basis.

15.2 Technical Platform Support includes platform training and enablement of MARINA staff on a request basis.

15.3 Technical Platform Support includes issue investigation

15.4 Technical Platform Support includes regular billing reporting and recommendations on cost reduction activities.

15.5 Technical Platform Support includes regular utilization reporting and recommendations on utilization optimization activities.

Severity Level	Description	Response Time
Severity 1 (Critical)	System outage or major disruption impacting critical services	15 minutes
Severity 2 (Major)	Significant impact on non-critical services or degradation of critical services	45 minutes
Severity 3 (Moderate)	Minor impact on services or functionality	120 minutes
Severity 4 (Low)	Cosmetic issues, minor bugs, or general inquiries.	24 hours

16. Other Services Includes:

- Monthly Consumption Reporting and Analysis
- 12x6 local support
- Managed Services:
 - Setup and Initial Deployment
 - Infrastructure Management and Maintenance
 - Fine-tune of WAF and Anti-DDoS

• Support / Monitoring

17. The subscription includes maintenance for one (1) year.

18. **As part of this engagement, the proposed solution shall include a comprehensive Knowledge Transfer and Training Program for MARINA personnel.** This program shall ensure that designated technical and administrative staff are fully equipped to effectively manage, monitor, and secure the cloud-hosted environment supporting MARINA-BEST.

The Knowledge Transfer and Training shall, at a minimum, cover the following:

- Cloud platform architecture and service components supporting MARINA-BEST
- System administration, monitoring, and performance optimization
- Cybersecurity controls, access management, and incident response procedures
- Data backup, redundancy, and disaster recovery mechanisms
- Best practices for system maintenance, compliance, and operational continuity

The training shall include **hands-on sessions, technical documentation, and operational guides**, and shall be conducted in a manner that ensures sustainability of system operations even after the completion of the contract.

This provision ensures that MARINA retains institutional knowledge, strengthens internal cybersecurity capability, reduces dependency on external providers, and supports long-term operational resilience of its digital maritime services.

Other Requirements

The following are the minimum qualifications and requirements for the Supplier or Bidder:

1. Track Record
 - 1.1 The service provider must be in the same industry as per their SEC/DTI filing for at least five (5) years.
 - 1.2 The service provider must be an operational company for at least ten (10) years.
 - 1.3 The service provider must have satisfactorily implemented a similar project within the last three (3) years. *(Please submit a copy of the certificate upon post-qualification)*
 - 1.4 The service provider must have at least two (2) years experience in providing cloud hosting subscription services in the public sector.
2. Organization
 - 2.1 The service provider must be filed with DTI or SEC as an IT company with the purpose of software development and the supply of IT-related goods and services.

	<p>2.2 Must have an updated National Privacy Commission (NPC) Certification with Data Privacy Officer.</p> <p>2.3 The Service Provider must have a verified specialization in cloud-based workforce productivity and digital transformation, or an equivalent field. The Service Provider must demonstrate expertise in delivering cloud infrastructure solutions for the public sector/government, with a proven track record of at least two (2) years. The Service Provider must also be authorized to provide and manage cloud security operations and infrastructure protection services from a Tier 1 Service Provider. In addition, the Service Provider must hold the highest tier of technical expertise (e.g., Premier, Elite, or Platinum) from the principal cloud provider. <u>(Please submit any proof of evidence or certificate upon post-qualification).</u></p> <p>2.4 The service provider must not have a history of blacklisting (or any recommendations towards such) in PhilGEPS as raised by any government agency in the past five (5) years.</p> <p>2.5 The service provider shall guarantee that the system shall abide with the DATA PRIVACY ACT of 20212 to ensure that the personal information is protected.</p> <p>2.6 The bidder must be an authorized direct reseller of the security solutions for the Cloud services being offered, and this should be clearly reflected in the bidder's cloud certification.</p>
Delivery Schedule	The implementation and/or activation is within thirty (30) days from the issuance of the Notice to Proceed.
Terms of Payment	The total contract price shall be paid in twelve (12) equal monthly installments upon submission of invoice/billing statement. The initial payment shall be made within fifteen (15) days upon issuance of Inspection and Acceptance Certificate.
Note: Prospective bidder must comply with all of the above requirements to become eligible with the said procurement project	

Prepared by:


ADRIAN G. RAMOS
 ITO II, MISS

Approved by:


JOSEPH VICTOR S. GENERATO, PhD
 Director II, MISS