TERMS OF REFERENCE

ANNUAL MAINTENANCE OF CLOUD-BASED DATA MANAGEMENT PLATFORM FOR DATA ANALYTICS PROJECT

The Bases Conversion and Development Authority (BCDA), a government instrumentality, seeks to procure an online data management platform that governs and manages all aspects of the data lifecycle that is vital to BCDA's operations through Small Value Procurement in accordance Republic Act No. 9184 and its revised Implementing Rules and Regulations.

Data management is a range of components and processes that work together to help the organization extract value from the data. These can include database management systems, data warehouses and lakes, data integration tools, visualization, analytics and more.

Objective

The project aims to help the organizations and employees connect things and optimize the use of data within the bounds of policy and regulation, provide meaningful and contextual cross-organizational information, enabling standardized and consistent access to datasets and enabling them to leverage their data effectively and make data-driven decisions.

This cloud initiative should also help the organization reduce costs in ICT acquisition and operation, achieve operational excellence, reduce security gaps, increase employee productivity, and develop excellent online services.

Project Scope Description

To implement the project, BCDA requires a cloud-based platform to manage all the data assets inventory of BCDA across different sources:

I. **The Approved Budget of the Contract (ABC) is One Million Pesos (Php 1,000,000.00), inclusive of all applicable taxes and fees.**

II. **General Requirements**

1. The SUPPLIER shall provide a cloud-based data management platform to cover data across different sources.
2. The SUPPLIER shall provide BCDA an access to a single-pane portal for multi-cloud management, catalogue, billing, and consumption monitoring with comprehensive business intelligence reports.
3. The SUPPLIER must provide the following certifications of the cloud solution:
    a. Solution Partner for Cloud Infrastructure
    b. Solution Partner for Data and AI
    c. Solution Partner for Security

        d. Solution Expert Managed Service Provider (MSP)
4.   The SUPPLIER must have at least one (1) Certified In-Country personnel of the cloud solution on any of the following:
        a. Data Engineer Associate
        b. Data Scientist Associate
        c. Business Intelligence Data Analyst Associate
5.   The SUPPLIER must have at least one (1) Certified In-Country personnel of the cloud solution for any of the following:
        a. Solutions Architect Expert
        b. DevOps Engineering Expert
        c. Cloud Expert
6.   The SUPPLIER must ensure that the cloud provider is one of Gartner's Top Two Cloud Infrastructure and Platform Services Leaders within the past two (2) years.
7.   The SUPPLIER must be on the highest partnership tier with the Cloud Service Providers specified in item no. II.6 above.
8.   The SUPPLIER must have at least one (1) Associate Level, or Higher Certification, for each of the top two (2) Cloud Services Providers.
9.   The SUPPLIER must provide the following ISO certifications:
        a. ISO/IEC 27701:2019
        b. ISO/IEC 27001:2017
10. The SUPPLIER shall provide cloud utilization reports upon the request of BCDA.
11. The SUPPLIER shall provide two (2) data visualization tool subscription licenses for one (1) year.
12. The SUPPLIER shall ensure that the cloud platform is compliant with the following minimum components, functionalities, and specifications:

CLOUD INFRASTRUCTURE

Cloud Hosting of Cloud Based Analytics Platform whose business functionalities shall be developed, implemented, and maintained by BCDA.
Supports selection of operating systems, frameworks, tools, databases, and devices such as but not limited to Linux and Windows Servers.
Supports SQL and Non-SQL databases.
Compliant with international and industry-specific standards.
Provide convenient access by different devices (e.g., server, desktop, Laptop, mobile, tablet, etc.).
Supports various forms of connectivity; secure and cross-premise connectivity with the virtual network and on-premises infrastructure.

Supports various forms of storage with different capabilities such as data recovery, security, backup, and protection.
Supports data migration.
Provides a Secure network with layers of authentication and organizational security.
Supports development of web and mobile applications that can be deployed to any platform or device e.g., build apps with JavaScript, Python, .NET, PHP, Java and Node.js; Build back-ends for iOS, Android, and Windows devices.
With test case execution and management.
Security must provide a wide array of configurable options and the ability to monitor, control, customize and increase security to meet BCDA's system deployments through built-in features and through partner solutions that can be deployed.
Support data durability – the ability to keep the stored data consistent, intact without the influence of failures or any form of corruption.
Support resource scalability – the ability for a resource (e.g., virtual machine) to scale vertically and horizontally.
Support for Platform as a Service (PAAS) – provides a platform allowing BCDA to develop, run and manage applications without the complexity of building and maintaining the infrastructure.
Supports capability to source, cleanse and transform unstructured data (real time, batch, and streaming).
Support for different types of workloads – provides multiple options in terms of compute, storage, database, networking, software, and intelligence for different types of workloads.
Support for measurement of service to automatically control and optimize use by leveraging a metering capability at some level of abstraction appropriate to the type of service.
Must have a financially backed service level agreement (SLA) that guarantees monthly availability.
Must have a facility to rapidly adjust usage of resources to match changing technical requirements.

Must have a gallery of predefined operating system and server software images for the rapid creation of operational Virtual Machines.
Supports the creation of virtual machines using a browser-based GUI.
Must have built in support for virtual networking and load balancing.
Must have built in facility for High Availability and Disaster Recovery Requirements.
Supports Virtual Private Network (VPN) to secure network traffic.
Must have a service that allows for a private dedicated connection to secure traffic.
Supports the rapid deployment and scaling of websites and web applications in minutes.
Supports server operating systems including Windows Server and Linux.
Supports multiple programming languages including JavaScript, Python, .NET, PHP, Java, and Node.js.
Supports Data Warehouse and analytics applications including SQL Server, Oracle, MySQL, Redis and MongoDB.
Must have a built-in facility to manage resources using templates for single click deployments of complex applications.
Must have the ability to orchestrate deployment using scripts and automation, aka Infrastructure as a Code (IaaC) by provisioning resources and other artifacts including role assignments, policy assignments and resource groups and resource managers.
Must have the ability to store in a central repository and use several types of secret/cryptographic keys data. (e.g., user credentials, certificates).
Must have a DNS hosting service which supports both private and public DNS. The DNS hosting service must be hosted on a global network of DNS servers, which answers a DNS query with the closest DNS server available.
Must provide preferential discounts for Virtual Machine services for securing longer term consumption and Bring Your Own License (BYOL) with corresponding software maintenance program.

CLOUD DATA STORAGE

No fixed limits on file size or account size.
Allows storage of unstructured and structured data in their native formats.
Provides massive throughput to increase analytic performance.
High durability, availability, and reliability.
Integrated access control support for cloud-based identity and authentication management solutions.
Option for Storage Tiering based on access frequency and/or content aging, providing cost optimization benefits, leveraging cloud scale and performance.
Option for a hierarchical file system that allows for more efficient data organization and management.
Seamless integration with other cloud infrastructure services.
Simplifies big data analytics by providing built-in data cloud governance.
Supports both file and object-based access.

INDUSTRY STANDARDS AND COMPLIANCE REQUIREMENTS OF THE CLOUD SOLUTION

Must have a facility for securely storing keys that is certified to FIPS 140-2 level 2 standard.
Must be certified on international and industry-specific compliance standards, including ISO 27001, ISO 22301, HIPAA, FedRAMP, SOC 1 Type 2 and SOC 2 Type 2, Australia IRAP, UK G-Cloud, Singapore MTCS, and ISO/IEC 27018.
Must be certified on ISO/IEC 27001/27002:2013 and ISO/IEC 27018:2014.
Must have passed the Content Delivery and Security Association (CDSA) audit for compliance with anti-piracy procedures governing digital media.
Must contractually conform to the Criminal Justice Information Services (CJIS) Security Policy of the Federal Bureau of Investigation (FBI).
Must comply with the security, privacy, compliance, and risk management requirements defined by the Cloud Security Alliance (CSA) in Cloud Controls Matrix (CCM) version 1.2.
Must have a DISA Provisional Authorization for Cloud Security Model Level 2 from the FedRAMP JAB which attests to compliance with required standards as dictated by DoD Instruction 8500.01 and 8510.01, the Security Requirements Guide, CDDSI 1253, and NIST 800-37/53.

Must provide contractual guarantees around transfer of personal data that conform to European Union (EU) Standard Contractual Clauses and approved by the EU's Article 29 Working Party for contractual commitments.
Must have a Provisional Authority to Operate from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board at a Moderate Impact level based upon the FIPS 199 classification.
Must comply with the framework published by the New Zealand (NZ) Government Chief Information Officer (GCIO) on the security and privacy aspects of cloud services.
Must comply with Payment Card Industry (PCI) Data Security Standards (DSS) Level 1 version 3.0.
Must comply with Section 508 that requires the publishing of Voluntary Product Accessibility Templates (VPAT) for cloud services.
Compliant with the Data Privacy Act of 2012.

III. Scope of Work

1. The SUPPLIER must maintain and provide consumable Credits for the following Cloud Resources:
   - Virtual Private Network Gateway for up to 730 Gateway Hours
   - Bandwidth of 500GB Internet Egress
   - 3 Static IP Addresses for 730 Hours
   - Inter-VNet Traffic (Peering) of up to 1TB
   - Platform Monitoring Service:
     - Daily Analytics Logs of 0.5GB
     - Daily Basic Logs of 0.5GB
   - Bastion for up to 730 Hours
   - Hierarchical File System to Support the Data Lake, with up to 256GB of Data Files

2. The SUPPLIER must provide the following:
   - Sixteen (16) hours Classroom-based training for up to ten (10) BCDA Personnel, for data analysis and visualization (*Training schedule must be within the contract period and agreed by both parties*):
     - Getting Started with Data Analytics
     - Data Preparation
     - Building Data Models
     - Creating Visuals and Reports
     - Managing Workspaces and datasets
     - Connecting various data sources
     - Clean and prepare data for analysis
     - Design Robust Data Models

- Certification Vouchers for up to ten (10) BCDA Personnel, for data analysis and visualization.
- Data Warehouse and Analytics Road Mapping Workshop.
- Two (2) data visualization tool subscription licenses for one (1) year from April 03, 2025 to April 02, 2026.

IV. Term and Effectivity

The engagement of this Cloud-based platform shall be for a period of one (1) year from March 22, 2025 to March 21, 2026.

The SUPPLIER shall be engaged to render services contracted to the Information and Communications Technology Department (ICTD) and shall report directly to the head of the department/unit or his duly authorized representative.

V. Delivery

The subscription and services of the Cloud-based platform and the data visualization tool subscription licenses shall be provided to BCDA upon the expiration of the current contract to assure the continuous accessibility of the platform and the data visualization tool.

The SUPPLIER shall demonstrate that the requirements specified by BCDA are properly provisioned and configured including all the necessary migration and customization if any.

VI. Terms of Payment

In consideration of the data management platform provided, BCDA agrees to pay the total amount of the project cost inclusive of all applicable taxes and fees. The consideration shall be paid under the following terms and conditions:

UPON COMPLETION OF THE FOLLOWING	
60% of the total project cost	Project Kick-off
	Data Warehouse and Analytics Road Mapping Workshop
	Provision of subscription and services of the Cloud-based platform
	Endorsement of Two (2) Licenses for Data Analysis and Visualization

30% of the total project cost	Sixteen (16) hours Classroom-based Data Analysis and Visualization Training for up to ten (10) BCDA Personnel
	Endorsement of Ten (10) Certification Vouchers for Data Analysis and Visualization
10% of the total project cost	Provision of Sign-off Documentation
	Acceptance by BCDA

Payment of billing shall be made within fifteen (15) calendar days from acceptance of the deliverables.

VII. Platform Security

BCDA and the SUPPLIER prioritize the security and integrity of data entrusted to the platform. Both parties acknowledge and adhere to the robust security measures of the platform.

The SUPPLIER shall ensure that data security measures adhere to the best practice recommendations provided by the Cloud Service Provider, as detailed on their official website. These measures should be implemented considering the applicability and feasibility within the end-customer's technical environment, as well as their compliance and security policies.

In the event of a suspected security breach or service degradation, the following procedures will be followed:

- Incident Reporting: BCDA will promptly report any suspected security breach or service degradation to the SUPPLIER through established channels.

- Investigation and Root Cause Analysis: The SUPPLIER, leveraging its expertise and advanced security tools, will conduct a thorough investigation to determine the root cause of the issue.

- Transparency and Communication: The SUPPLIER will maintain open communication with BCDA throughout the investigation, providing regular updates and detailed reports on the progress and findings.

- Remediation and Service Credits: If the investigation confirms a service degradation attributable to the platform and falling below the thresholds, BCDA will be eligible for service credits as per SUPPLIER's Service Level Agreement for Online Services.

  Additionally, the SUPPLIER will promptly implement remedial measures to mitigate the impact and prevent future occurrences.

- Focus on Data Security and Integrity: Regardless of the service availability outcome, the SUPPLIER's primary focus will remain on ensuring the utmost data security and preventing any unauthorized access or compromise of BCDA's data within the platform.

VIII. Service Level Agreement

The SUPPLIER shall provide the following support items for the duration of the contract:

1. Assistance and guidance on the cloud solution.
2. Web or Email support on break/fix incidents during business hours (Monday to Friday).
3. Billing and Account Management support.
4. 24/7 self-help resources to learning materials, how to videos, documentation, and community support.
5. In the case that there will be scheduled maintenance on the platform, the SUPPLIER shall notify the BCDA through email one (1) week in advance of scheduled maintenance.

IX. Warranty Security

Section 62.1 of the revised Implementing Rules and Regulations of R.A. 9184

For the procurement of Goods, in order to assure that manufacturing defects shall be corrected by the supplier, a warranty security shall be required from the contract awardee for a minimum period of three (3) months, in the case of Expendable Supplies, or a minimum period of one (1) year, in the case of Non-expendable Supplies, after acceptance by the Procuring Entity of the delivered supplies.

The obligation for the warranty shall be covered by either retention money in an amount equivalent to at least one percent (1%) but not to exceed five percent (5%) of every progress payment, or a special bank guarantee equivalent to at least one percent (1%) but not to exceed five percent (5%) of the total contract price. The said amounts shall only be released after the lapse of the warranty period or, in the case of Expendable Supplies, after consumption thereof: Provided, however, that the supplies delivered are free from patent and latent defects and all the conditions imposed under the contract have been fully met.

For the procurement of BCDA cloud-based data management platform project, which are neither expendable or non-expendable supplies, the BCDA will not require a Warranty Security.

Prepared by:

CORNELIO J. MARTIN III
IT Officer II
ICTD-ITD

MA. LUISA M. RODRIGUEZ
IT Officer III
ICTD-ITD

Recommended by:

VIRGIL M. ALVAREZ
Vice President
ICTD

Approved by:

ATTY. ELVIRA V. ESTANISLAO
Senior Vice President
Corporate Services Group