



REPUBLIC OF THE PHILIPPINES  
DEPARTMENT OF BUDGET AND MANAGEMENT  
GENERAL SOLANO STREET, SAN MIGUEL, MANILA

**SUPPLEMENTAL/BID BULLETIN (SBB) NO. 1**

This SBB No. 1 dated June 11, 2024, for **Project ID No. DBM-2024-57, “Subscription to Immutable and Verifiable Attributes (Blockchain) for the Department of Budget and Management Action Document Releasing System (ADRS),”** is issued pursuant to Section 22.5 of the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184, to clarify, modify or amend items in the Bidding Documents. Accordingly, this shall form an integral part of the Bidding Documents.

PARTICULAR(S)/QUERY(IES)			AMENDMENT(S)/CLARIFICATION(S)		
<p><b>Section VI. Schedule of Requirements</b></p> <p>The delivery schedule stipulates hereafter the date of delivery to the project site.</p>			<p><b>Section VI. Schedule of Requirements (REVISED)</b></p> <p>The delivery schedule stipulates hereafter the date of delivery to the project site.</p>		
Item	Description	Delivery Schedule	Item	Description	Delivery Schedule
1	<p><b>Deployment and installation of an online subscription to a cloud-computing platform,</b> as detailed in item 4.0 and 5.0 of Annex “A” (Detailed Technical Specifications) of Section VII. Technical Specifications.</p>	<p>Within thirty (30) calendar days from the issuance of the Notice to Proceed</p>	1	<p><del>Deployment and installation</del> <b>SET-UP, INSTALLATION, AND CONFIGURATION of an online subscription to a cloud-computing platform,</b> as detailed in item 4.0 and 5.0 of Annex “A” (Detailed Technical Specifications) of Section VII. Technical Specifications.</p>	<p>Within thirty (30) calendar days from the issuance of the Notice to Proceed</p>
2	<p><b>Subscription to Immutable and Verifiable Attributes (Blockchain),</b> as detailed in Annex “A” (Detailed Technical Specifications) of Section VII. Technical Specifications</p>	<p>Twelve (12) months from the issuance of Certificate of Acceptance after the deployment and installation of an online subscription to a cloud-computing platform</p>	2	<p><b>Subscription to Immutable and Verifiable Attributes (Blockchain),</b> as detailed in Annex “A” (Detailed Technical Specifications) of Section VII. Technical Specifications</p>	<p>Twelve (12) months from the issuance of <del>Certificate</del> <b>PROOF OF SUBSCRIPTION.</b> THE PROOF OF SUBSCRIPTION WILL ONLY BE ISSUED AFTER THE COMPLETE</p>

PARTICULAR(S)/QUERY(IES)	AMENDMENT(S)/CLARIFICATION(S)	
		SET UP, INSTALLATION, AND CONFIGURATION <del>after the deployment</del> <del>and installation of an</del> THE online subscription to a cloud-computing platform
<p align="center"><b>Section VII. Technical Specifications</b></p> <p align="center">xxx</p> <p><b>3.0 SUBSCRIPTION PERIOD</b></p> <p>The subscription period for the project shall be for twelve (12) months from the issuance of Certificate of Acceptance after the deployment and installation of online subscription to a cloud-computing platform.</p> <p align="center">xxx</p> <p><b>5.0 PROVISION OF TECHNICAL SUPPORT</b></p> <p>The Subscription to Immutable and Verifiable Attributes (Blockchain) for the Department of Budget and Management Action Document Releasing System (ADRS) shall include the following technical support services from the Contractor during the duration of the contract:</p> <p align="center">xxx</p> <p><b>6.0 TECHNICAL SUPPORT DEPLOYMENT TO DBM</b></p> <p align="center">xxx</p>	<p align="center"><b>Section VII. Technical Specifications (REVISED)</b></p> <p align="center">xxx</p> <p><b>3.0 SUBSCRIPTION PERIOD</b></p> <p>The subscription period for the project shall be for twelve (12) months from the issuance of <del>Certificate of Acceptance</del> <b>THE PROOF OF SUBSCRIPTION.</b> <b>THE PROOF OF SUBSCRIPTION WILL ONLY BE ISSUED AFTER THE COMPLETE SET UP, INSTALLATION, AND CONFIGURATION</b> <del>after the deployment and installation</del> of THE online subscription to a cloud-computing platform.</p> <p align="center">xxx</p> <p><b>5.0 <del>PROVISION OF TECHNICAL SUPPORT</del> SCOPE OF WORK</b></p> <p><del>The Subscription to Immutable and Verifiable Attributes (Blockchain) for the Department of Budget and Management Action Document Releasing System (ADRS) shall include the following technical support services from the Contractor during the duration of the contract:</del></p> <p align="center">xxx</p> <p><b>6.0 PROVISION OF TECHNICAL SUPPORT DEPLOYMENT TO DBM</b></p> <p><b>THE SUBSCRIPTION TO IMMUTABLE AND VERIFIABLE ATTRIBUTES (BLOCKCHAIN) FOR THE DEPARTMENT OF BUDGET AND MANAGEMENT ACTION DOCUMENT RELEASING SYSTEM (ADRS) SHALL</b></p>	

PARTICULAR(S)/QUERY(IES)	AMENDMENT(S)/CLARIFICATION(S)												
<p><b>7.0 SERVICE LEVEL AND SUBSCRIPTION AGREEMENT</b></p> <p>7.1. DBM shall maintain a Service Level Agreement (SLA) <b>xxx</b></p> <table border="1" data-bbox="121 880 783 1249"> <thead> <tr> <th>Component</th> <th>Description</th> <th></th> </tr> </thead> <tbody> <tr> <td>Delivery</td> <td>The CONTRACTOR shall deliver the following Software Licenses &amp; Platform with 1 Year Software Assurance within 15 calendar days from the issuance of Notice to Proceed (NTP) – Ready to integrate to ADRS and upload DBM actionable document.</td> <td>xxx</td> </tr> </tbody> </table> <p style="text-align: center;"><b>xxx</b></p> <p><b>11.0 TERMS OF PAYMENT</b></p> <p style="text-align: center;"><b>xxx</b></p> <p>11.2. Payment shall be made within a reasonable time from the submission of the documentary requirements such as, but not limited to the following, based on existing accounting and auditing laws, rules and regulations:</p> <ul style="list-style-type: none"> <li>i. Sales Invoicing/Billings</li> <li>ii. Certificate of Acceptance issued by ICTSS Director</li> <li>iii. Non-Disclosure Agreement</li> </ul> <p style="text-align: center;"><b>xxx</b></p>	Component	Description		Delivery	The CONTRACTOR shall deliver the following Software Licenses & Platform with 1 Year Software Assurance within 15 calendar days from the issuance of Notice to Proceed (NTP) – Ready to integrate to ADRS and upload DBM actionable document.	xxx	<p><b>INCLUDE THE FOLLOWING TECHNICAL SUPPORT SERVICES FROM THE CONTRACTOR DURING THE DURATION OF THE CONTRACT:</b></p> <p>6.1 The contractor shall deploy the following technical personnel to provide technical support to the DBM:</p> <p style="text-align: center;"><b>xxx</b></p> <p><b>7.0 SERVICE LEVEL AND SUBSCRIPTION AGREEMENT</b></p> <p>7.1. DBM shall maintain a Service Level Agreement (SLA) <b>xxx</b></p> <table border="1" data-bbox="813 880 1476 1249"> <thead> <tr> <th>Component</th> <th>Description</th> <th></th> </tr> </thead> <tbody> <tr> <td>Delivery</td> <td>The CONTRACTOR shall deliver the following Software Licenses &amp; Platform with 1 Year Software Assurance within <del>15</del> <b>30</b> calendar days from the issuance of Notice to Proceed (NTP) – Ready to integrate to ADRS and upload DBM actionable document.</td> <td>xxx</td> </tr> </tbody> </table> <p style="text-align: center;"><b>xxx</b></p> <p><b>11.0 TERMS OF PAYMENT</b></p> <p style="text-align: center;"><b>xxx</b></p> <p>11.2. Payment shall be made within a reasonable time from the submission of the documentary requirements such as, but not limited to the following, based on existing accounting and auditing laws, rules and regulations:</p> <ul style="list-style-type: none"> <li>i. Sales Invoicing/Billings</li> <li>ii. Certificate of Acceptance issued by <del>ICTSS Director</del> <b>THE UNDERSECRETARY OF THE ICT GROUP/CHIEF INFORMATION OFFICER.</b></li> <li>iii. Non-Disclosure Agreement</li> <li>iv. <b>PROOF OF SUBSCRIPTION</b></li> </ul>	Component	Description		Delivery	The CONTRACTOR shall deliver the following Software Licenses & Platform with 1 Year Software Assurance within <del>15</del> <b>30</b> calendar days from the issuance of Notice to Proceed (NTP) – Ready to integrate to ADRS and upload DBM actionable document.	xxx
Component	Description												
Delivery	The CONTRACTOR shall deliver the following Software Licenses & Platform with 1 Year Software Assurance within 15 calendar days from the issuance of Notice to Proceed (NTP) – Ready to integrate to ADRS and upload DBM actionable document.	xxx											
Component	Description												
Delivery	The CONTRACTOR shall deliver the following Software Licenses & Platform with 1 Year Software Assurance within <del>15</del> <b>30</b> calendar days from the issuance of Notice to Proceed (NTP) – Ready to integrate to ADRS and upload DBM actionable document.	xxx											

PARTICULAR(S)/QUERY(IES)	AMENDMENT(S)/CLARIFICATION(S)
	<b>xxx</b>
<p><b>Queries:</b></p> <ol style="list-style-type: none"> <li>1. Explain the requirement on the Data Analytics and Artificial Intelligence.</li>   <li>2. Please provide workflow of documents for the use case given its linkage to the Document System.</li>   <li>3. What is the volume of transactions on daily basis or monthly basis?</li>   <li>4. Was a Proof of Concept (POC) done/completed How was the preparation? What is the scope and the results?</li> </ol>	<p><b>Clarifications:</b></p> <ol style="list-style-type: none"> <li>1. The requirements for Data Analytics and Artificial Intelligence are outlined in Item 4.1.3 of Annex A of Section VII. Technical Specifications (Revised). Specifically, the contractor’s cloud platform must provide AI services and cognitive APIs as Platform as a Service (PaaS) with additional functionalities stated in the afore-cited section.  The cloud platform, among others, should have AI capabilities and cognitive APIs that will allow DBM to access and integrate the platform into other existing systems or future projects that will be linked to the Action Document Releasing System (ADRS) and ensure interoperability.</li>   <li>2. The initial application of blockchain technology in the public sector, specifically within the Department of Budget and Management (DBM), will be in the ADRS.  Blockchain technology will enhance the immutability and verifiability of records posted in the ADRS, including disbursement and obligational authorities issued by the DBM, which serve as the official basis for the release of funds.</li>   <li>3. The volume of transactions is relative based on the operations of the DBM. Based on the Section VII. Technical Specifications (Revised), the DBM shall be allowed to upload all the documents (maximum of 500,000 upload in one (1) year) using a blockchain as a service with Private, Public and Hybrid Accountability Ledger.</li>   <li>4. Yes, it had a POC where a prototype was completed to cover identified action documents such as the Special Allotment Release Order (SARO) and Advice of Notice of Cash Allocation Issued (ANCAI).</li> </ol>

PARTICULAR(S)/QUERY(IES)	AMENDMENT(S)/CLARIFICATION(S)
<p>5. Will the tender include support? Will we provide the costing for yearly support?</p> <p>6. Most of the companies providing blockchain software are from the outside the Philippines, such as in the US and Singapore. However, one of the requirements to participate in the bidding process is that a company must be registered in the Philippines. How can foreign companies participate in the bidding?</p>	<p>5. Yes. Under Section VII. Technical Specifications (Revised), the contractor shall provide technical support to DBM. This shall be included in the total cost for the project.</p> <p>6. In relation to the eligibility to participate in THE public bidding activities of the DBM, the applicable law provides that only Filipino citizens identified under Section 23.4.1 of the Revised IRR of RA No. 9184 may participate. By way of exception, foreign bidders may be eligible to participate under any of the following circumstances in accordance with the guidelines issued by the GPPB:</p> <ul style="list-style-type: none"> <li>a) When provided for under any Treaty or International or Executive Agreement as provided in Section 4 of the Act and this IRR;</li> <li>b) When the foreign supplier is a citizen, corporation or association of a country, the laws or regulations of which grant reciprocal rights or privileges to citizens, corporations or associations of the Philippines;</li> <li>c) When the goods sought to be procured are not available from local suppliers; or</li> <li>d) When there is a need to prevent situations that defeat competition or restrain trade.</li> </ul> <p>On the other hand, Section 23.4.1.1(e) of the Revised IRR of RA No. 9184, persons/entities forming themselves into a joint venture, i.e., a group of two (2) or more persons/entities that intend to be jointly and severally responsible or liable for a particular contract, shall be allowed to participate in the bidding for the supply of goods. It mandates, however, that Filipino ownership or interest of the joint venture concerned shall be at least sixty percent (60%). For this purpose, Filipino ownership or interest shall be based on the contributions of each of the members of the joint venture as specified in their JVA.</p>

PARTICULAR(S)/QUERY(IES)	AMENDMENT(S)/CLARIFICATION(S)
<p>7. Is there a limit on the number of bidders?</p> <p>8. Our company is an interested Bidder for this ITB, so could you please let us know if it is still possible for us to acquire a complete set of Bidding Documents for this purchase procedure? If yes - please let me know about it.</p>	<p>7. None. There is no prescribed limit on the number of bidders who can participate in the bidding process.</p> <p>8. Pursuant to Item 5 of the Invitation to Bid, the complete set of Bidding Documents may be acquired by interested Bidders beginning May 28, 2024 from the given address and website below and upon payment of a fee in the amount of Ten Thousand Pesos (P10,000.00).</p> <p>For further information, please refer to:  DBM-BAC Secretariat  DBM-Administrative Service-Procurement Management Division  Ground Floor, DBM Building III, General Solano St., San Miguel, Manila  Telefax No. 8657-3300 local 3115  Email address: <a href="mailto:procurement@dbm.gov.ph">procurement@dbm.gov.ph</a></p> <p>You may visit the following website to download the Bidding Documents:  <a href="https://www.dbm.gov.ph/index.php/procurement/invitation-to-bid">https://www.dbm.gov.ph/index.php/procurement/invitation-to-bid</a></p>
	<p><b>Note:</b></p> <p><b><u>Attached are the following documents which should be used as part of the Bidding Documents to be submitted by the bidders:</u></b></p> <ol style="list-style-type: none"> <li><b>1. Section VI. Schedule of Requirements (Revised); and</b></li> <li><b>2. Section VII. Technical Specifications (Revised)</b></li> </ol>

**Other matters:**

- The “No Contact Rule” shall be strictly observed. Bidders are not allowed to communicate with any member of the Bids and Awards Committee, Technical Working Group or Secretariat effective June 18, 2024, right after the opening of bids.
  
- For guidance and information of all concerned.

**RAMON VICENTE B. ASUNCION**

*Acting Assistant Secretary and Concurrent Director IV*

*Vice Chairperson, DBM-BAC*

## ***Section VI. Schedule of Requirements (Revised)***

The delivery schedule stipulates hereafter the date of delivery to the project site.

<b>Item</b>	<b>Description</b>	<b>Delivery Schedule</b>
<b>1</b>	<b>Set-up, installation and configuration of an online subscription to a cloud-computing platform</b> , as detailed in item 4.0 and 5.0 of Annex “A” (Detailed Technical Specifications) of Section VII. Technical Specifications.	Within thirty (30) calendar days from the issuance of the Notice to Proceed
<b>2</b>	<b>Subscription to Immutable and Verifiable Attributes (Blockchain)</b> , as detailed in Annex “A” (Detailed Technical Specifications) of Section VII. Technical Specifications	Twelve (12) months from the issuance of Proof of Subscription. The Proof of Subscription is issued only after the complete set up, installation, and configuration of the online subscription to a cloud-computing platform

**I hereby certify to comply and deliver all the above requirements.**

\_\_\_\_\_  
Name of Company/Bidder

\_\_\_\_\_  
Signature Over Printed Name of Representative

\_\_\_\_\_  
Date



## ***Section VII. Technical Specifications (Revised)***

Bidders must state here either “Comply” or any equivalent term in the column “Bidder’s Statement of Compliance” against each of the individual parameters of each “Specification.”

<b>Specifications</b>	<b>Bidder’s Statement of Compliance</b>
<b>I. Subscription Period</b> <i>(see attached Annex “A” [Detailed Technical Specifications], item 3.0)</i>	
<b>II. Specifications and Platform Capability</b> <i>(see attached Annex “A” [Detailed Technical Specifications], item 4.0)</i>	
<b>III. Scope of Work</b> <i>(see attached Annex “A” [Detailed Technical Specifications], item 5.0)</i>	
<b>IV. Provision of Technical Support to DBM</b> <i>(see attached Annex “A” [Detailed Technical Specifications], item 6.0)</i>	
<b>V. Service Level and Subscription Agreement</b> <i>(see attached Annex “A” [Detailed Technical Specifications], item 7.0)</i>	
<b>VI. Qualifications of the Contractor</b> <i>(see attached Annex “A” [Detailed Technical Specifications], item 8.0)</i>	
<b>VII. Confidentiality of Data</b> <i>(see attached Annex “A” [Detailed Technical Specifications], item 9.0)</i>	
<b>VIII. Warranties of the Contractor</b> <i>(see attached Annex “A” [Detailed Technical Specifications], item 10.0)</i>	
<b>IX. Terms of Payment</b> <i>(see attached Annex “A” [Detailed Technical Specifications], item 11.0)</i>	

<p><b>X. Pre-Termination of Contract</b>  <i>(see attached Annex "A" [Detailed Technical Specifications], item 12.0)</i></p>	
--	--

**I hereby certify to comply with all the above Technical Specifications.**

\_\_\_\_\_  
**Name of Company/Bidder                      Signature Over Printed Name of Representative                      Date**

## **Detailed Technical Specifications**

### **1.0 PROJECT TITLE**

Subscription to Immutable and Verifiable Attributes (Blockchain) for the Department of Budget and Management Action Document Releasing System (ADRS)

### **2.0 OBJECTIVE**

This project aims to leverage the benefits of both private and public blockchain technologies to enhance transparency, efficiency, and accountability in digital document processing. The primary objective is to use blockchain as the point of truth of a specific document, enabling seamless tracking and verification.

### **3.0 SUBSCRIPTION PERIOD**

The subscription period for the project shall be for twelve (2) months from the issuance of the Proof of Subscription. The Proof of Subscription will only be issued after the complete set up, installation, and configuration of the online subscription to a cloud-computing platform.

### **4.0 SPECIFICATIONS AND PLATFORM CAPABILITY**

#### **4.1. CONTRACTOR’S PLATFORM CAPABILITY**

##### **4.1.1. General Requirements**

- 4.1.1.1. The CONTRACTOR must supply an online subscription to the cloud-computing platform and shall be made available 24/7 to the authorized users of DBM throughout the entire duration of the project.
- 4.1.1.2. The CONTRACTOR must supply MS SQL Database Ledger, other databases, and confidential ledger.
  - 4.1.1.2.1. The solution provides confidential ledger that runs on minimalistic trusted.
  - 4.1.1.2.2. The solution must support both public and private ledger types.
- 4.1.1.3. The CONTRACTOR’s cloud platform must comply with Payment Card Industry (PCI) Data Security Standards (DSS) Level 1 version 3.0 and PCI 3DS.

- 4.1.1.4. The CONTRACTOR's cloud platform must support various forms of storage with different capabilities such as data recovery, disk replication, security, backup, and protection.
- 4.1.1.5. The CONTRACTOR's cloud platform security must provide a wide array of configurable options and the ability to monitor, control, customize and increase security to meet DBM's system deployments through native cloud service features.
- 4.1.1.6. The CONTRACTOR's cloud platform must have support for different types of workloads and multiple options in terms of computing including virtual desktops with personal and multi session capability.
- 4.1.1.7. The CONTRACTOR's cloud platform must have support for multi-cloud management environment from a Single Pane of Glass to implement consistent inventory, management, governance, and security for servers across the environment.
- 4.1.1.8. The CONTRACTOR's cloud platform must integrate into the existing Azure Entra ID (Active Directory) Tenant used for the existing M365 Environment.
- 4.1.1.9. The CONTRACTOR's cloud platform must provide preferential discounts for Virtual Machine services for securing longer term consumption and Bring Your Own License (BYOL) w/ Software Assurance.

#### 4.1.2. **Security**

- 4.1.2.1. The CONTRACTOR's cloud platform must provide a cloud-native unified security management platform that includes the following features:
  - 4.1.2.1.1. Security health monitoring for cloud;
  - 4.1.2.1.2. Cloud Security Posture Management;
  - 4.1.2.1.3. Protect the cloud-native resources including a secure score to assess the current security situation;
  - 4.1.2.1.4. Continually compare the configuration of your resources with requirements in industry standards, regulations, and benchmarks where applicable;
  - 4.1.2.1.5. Security threat blocking through access and app controls;
  - 4.1.2.1.6. Adjustable security policies for maintaining regulatory and standard compliance;

- 4.1.2.1.7. Security vulnerability discovery tools and patches;
  - 4.1.2.1.8. Advanced threat detection through security alerts and analytics;
  - 4.1.2.1.9. The solution should have capability for Attack path analysis that helps you to address the security issues that pose immediate threats with the greatest potential of being exploited in your environment;
  - 4.1.2.1.10. Agentless scanning to assist in the identification process of actionable posture issues without the need for installed agents, network connectivity, or any effect on machine performance;
  - 4.1.2.1.11. The solution can query all security issues and environment context such as assets inventory, exposure to internet, permissions, and lateral movement between resources and across multiple clouds; and
  - 4.1.2.1.12. Can periodically analyze the security state of resources connected to subscriptions to identify potential security issues and provide active recommendations. Active recommendations are recommendations that can be resolved to improve your security posture.
    - 4.1.2.1.12.1. The solution should provide contextual security capabilities that assist security teams in the reduction of the risk of impactful breaches and context to perform a risk assessment of DBM's cloud security issues.
- 4.1.2.2. The cloud infrastructure should have Cloud Workload Protection capabilities below:
- 4.1.2.2.1. Cloud-native application protection platform (CNAPP) that is made up of security measures and practices that are designed to protect cloud-based applications from various cyber threats and vulnerabilities;
  - 4.1.2.2.2. The solution should have threat detection and advanced defenses to Windows and Linux machines that run in existing DBM Cloud Platforms, and on premises;
  - 4.1.2.2.3. Supports an agentless malware scanning capability that scans and detects malware and viruses. The

scanner is available for Azure virtual machines (VM), AWS EC2 instances and GCP VM instances;

- 4.1.2.2.4. The agentless scanner scans all files and folders including any files or folders that are excluded from the agent-based antivirus scans, without having an effect on the performance of the machine;
  - 4.1.2.2.5. The solution protection should have capabilities for Discover vulnerabilities and misconfigurations in near real time;
  - 4.1.2.2.6. Prioritize vulnerabilities based on the threat landscape and detections in the organization;
  - 4.1.2.2.7. Holistic, cloud-delivered, endpoint security solution;
  - 4.1.2.2.8. Risk-based vulnerability management and assessment:
    - 4.1.2.2.8.1. Attack surface reduction;
    - 4.1.2.2.8.2. Behavioral based and cloud-powered protection
    - 4.1.2.2.8.3. Endpoint detection and response (EDR);
    - 4.1.2.2.8.4. Automatic investigation and remediation;
    - 4.1.2.2.8.5. Managed hunting services;
  - 4.1.2.2.9. Risk-based vulnerability management and assessment;
  - 4.1.2.2.10. The solution includes File Integrity Monitoring (FIM) examines operating system files, Windows registries, application software, and Linux system files for changes that might indicate an attack; and
  - 4.1.2.2.11. The solution can lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
- 4.1.2.3. The solution is capable for User and Entity Behavior Analytics (UEBA), which collects logs and alerts from all its connected data sources, it analyzes them and builds baseline behavioral profiles of

the organization's entities (such as users, hosts, IP addresses, and applications) across time and peer group horizon.

- 4.1.2.3.1. Data Sources- thoughtfully selects third-party data sources to provide data that matches the threat scenarios.
- 4.1.2.3.2. Analytics: Using various machine learning (ML) algorithms, able to identify anomalous activities and presents evidence clearly and concisely in the form of contextual enrichments.
- 4.1.2.4. The solution must come with connectors for any data sources that are available out-of-the-box and provide real-time integration. Also support common event format (CEF), Syslog or REST-API to connect data sources and which allows for easy integration with third-party security tools and services.
- 4.1.2.5. The solution should provide an option to export stored data for long-term retention and:
  - 4.1.2.5.1. The solution should provide built-in SOAR (Security Orchestration, Automation & Response) capability and ability to create playbooks;
  - 4.1.2.5.2. Supporting "no code" methods for rapid playbook creation supporting easy decision making and branching capabilities;
  - 4.1.2.5.3. Support prebuilt design templates;
  - 4.1.2.5.4. Code based logic like JSON, etc.;
  - 4.1.2.5.5. Support out-of-the-box connectors to save playbook creation time; and
  - 4.1.2.5.6. Support export of playbooks and reuse it.
- 4.1.2.6. The SIEM should have the capability to seamlessly integrate with the existing Microsoft 365, utilizing XDR for identity, email, endpoint, and multi-cloud functions. Additionally, it should be able to ingest log sources at no extra cost.
- 4.1.2.7. It should also possess the capability to implement and integrate with an AI tool for enhancing threat detection and response, as well as enabling forensic investigation in the future.

### 4.1.3. Data Analytics and Artificial Intelligence

4.1.3.1. The CONTRACTOR's cloud platform must provide AI services and cognitive APIs as Platform as a Service (PaaS) with additional functionalities stated below:

4.1.3.1.1. Must provide pre-built models for decision, language, speech, vision, forms recognition, metrics advisor:

4.1.3.1.1.1. Must support REST API;

4.1.3.1.1.2. Must have container support; and

4.1.3.1.1.3. Must have SDK for programming languages (e.g., .NET, Node.js, Python, Java, Go);

4.1.3.1.2. Must provide Generative Pre-trained Transformers (GPT) large language models (LLM):

4.1.3.1.2.1. Transformer models must deliver natural language understanding and generation and are fine-tuned to be capable of function calls based on the context of prompts;

4.1.3.1.2.2. Transformer models must deliver image generation from natural language descriptions, and support code understanding and generation; and

4.1.3.1.2.3. Transformer models must support embeddings for similarity, text search, and code search functionalities;

4.1.3.1.3. Must have a layered security model:

4.1.3.1.3.1. Must be able to limit access to specific subset of networks allowing requests originating from specified private IP addresses, private IP ranges or from list of private subnets;

4.1.3.1.3.2. Must support authorization through Azure Active Directory (AAD) or equivalent Identity and Access Management (IAM) provider; and



- 4.1.3.1.3.3. Must support custom subdomain names for endpoints;
- 4.1.3.2. DBM user prompts or embeddings will not be used to improve the Cloud Service Provider or other 3rd party products or services;
- 4.1.3.3. DBM data from any fine-tuning is not used by the Cloud Service Provider to train Large Language Models;
- 4.1.3.4. CONTRACTOR's Cloud platform for LLM allows encryption with Customer Managed Keys;
- 4.1.3.5. CONTRACTOR's Cloud platform should include risk mitigation or content filtering that detects and prevents the output of harmful content such as self-harm, hate, sexual or violence; and
- 4.1.3.6. CONTRACTOR's Cloud platform upholds responsible AI principles in their company and practices governance, rules, training, and tools to operationalize those principles.

#### 4.1.4. **DevOps**

- 4.1.4.1. The CONTRACTOR's Cloud platform must provide DevOps functionality as Platform as a Service (PaaS) with additional functionalities stated below:
  - 4.1.4.1.1. Software development platform editor that must have an AI plug-in that serves as a pair programmer:
    - 4.1.4.1.1.1. The plug-in must turn natural language prompts into code in real-time;
    - 4.1.4.1.1.2. The plug-in offers multi-line function suggestions;
    - 4.1.4.1.1.3. The plug-in can generate unit tests from code
    - 4.1.4.1.1.4. The plug-in filters out common vulnerable coding patterns;
    - 4.1.4.1.1.5. The plug-in blocks suggestions matching public code; and
    - 4.1.4.1.1.6. The plug-in autofill's repetitive codes.
- 4.1.4.2. The CONTRACTOR's Cloud platform must be recognized and included in the 2023 Gartner Leaders for DevOps Platform.

## **4.2. CONTRACTOR’S INFRASTRUCTURE SPECIFICATIONS**

- 4.2.1. The CONTRACTOR’s platform should be provided for a minimum of one (1) year of subscription with the following specification once deployed:
  - 4.2.1.1. Should be under a Blockchain Chain as a Service model with Web API; and
  - 4.2.1.2. Should be Public and Private blockchain connected with an accountability ledger with head/line pattern:
    - 4.2.1.2.1. Must host 500,000 combined private and public blockchain transaction documents.

## **5.0 SCOPE OF WORK**

### **5.1. Private Blockchain**

- 5.1.1. Leverage Confidential Ledger's advanced privacy features to create a secure and tamper-resistant private blockchain network.
- 5.1.2. Ensure that only authorized participants, such as government agencies and DBM staff, can access and transact on the private blockchain.
- 5.1.3. Design the network architecture, consensus mechanism, access controls, and permission models to establish a robust and scalable private blockchain infrastructure.
- 5.1.4. Utilize private blockchain privacy-enhancing technologies to protect sensitive budgetary information and maintain the confidentiality of transactions.

### **5.2. Public Blockchain**

- 5.2.1. Utilize Layer 2, a public blockchain platform, to enhance transparency and accountability in the budgeting process. (Layer 2 [L2] solutions are secondary frameworks built on top of existing blockchain networks [Layer 1] to increase transaction speed and reduce costs, without sacrificing security. These solutions work by processing transactions off the main blockchain, in a manner that is still anchored to the main chain, ensuring the integrity and security of transactions. By integrating L2 solutions into budgeting processes, organizations can leverage these fast, cost-effective, and secure platforms to ensure greater transparency and accountability, making operations more efficient and trustworthy.)
- 5.2.2. Leverage proof-of-stake consensus mechanism to ensure fast transaction processing, scalability, and energy efficiency.
- 5.2.3. Integrate the private blockchain with the public blockchain to enable public auditability and verification of token transactions and budget allocation.

- 5.2.4. Design and implement smart contracts on the public blockchain to facilitate the transparent and auditable distribution of tokenized budget appropriations.
- 5.2.5. Must use zero knowledge proof or anonymized transaction as extra added security.

### **5.3. Hybrid Accountability Ledger**

Conduct a comprehensive assessment of the DBM's existing documentation processes to identify areas that can benefit from blockchain technology. Engage stakeholders, including government agencies and subject matter experts, to gather requirements and understand their needs and expectations.

### **5.4. Requirements Gathering**

- 5.4.1. Conduct a comprehensive assessment of the DBM's existing documentation processes to identify areas that can benefit from blockchain technology.
- 5.4.2. Engage stakeholders, including government agencies and subject matter experts, to gather requirements and understand their needs and expectations.

### **5.5. Private Blockchain Development**

- 5.5.1. Design and develop a private blockchain network on confidential ledger.
- 5.5.2. Define the network architecture, consensus mechanism, access controls, and permission models for the private blockchain.
- 5.5.3. Ensure interoperability with existing systems and data sources.

### **5.6. Public Blockchain Integration**

- 5.6.1. Investigate and select the most suitable public blockchain platform, such as Layer 2 PoS (Proof of Stake), for integration with the private blockchain.
- 5.6.2. Design and develop smart contracts on the public blockchain to enable transparent and auditable token transactions and budget allocation.

### **5.7. Unique Identifier Framework (UID)**

- 5.7.1. Create a comprehensive framework for budget documents with UID on the combined private and public blockchain.
- 5.7.2. Define the rules, smart contracts, and business logic for generating, distributing, and tracking tokens representing allocated funds to government agencies.
- 5.7.3. Ensure the accuracy, reliability, and traceability of token transactions.
- 5.7.4. Should have built Inscription Model for Certificate of Authenticity in a layer 2 blockchain.

## **5.8. User Interface and Reporting**

- 5.8.1. Design and implement user-friendly interfaces for government agencies and DBM staff to interact with the blockchain platform.
- 5.8.2. Provide real-time reporting and analytics capabilities to monitor token transactions, budget utilization, and performance.
- 5.8.3. Ensure accessibility and ease of use for all stakeholders.

## **5.9. Security and Governance**

- 5.9.1. Implement robust security measures to safeguard the private and public blockchain networks.
- 5.9.2. Establish governance mechanisms, consensus protocols, access controls, and auditing processes.
- 5.9.3. Define roles and responsibilities for network participants and administrators to ensure compliance with relevant regulations.

## **5.10. Training and Capacity Building**

- 5.10.1. Conduct training programs and workshops to educate government agencies and DBM staff on the functionalities, benefits, and usage of the blockchain platform.
- 5.10.2. Develop comprehensive documentation and training materials to facilitate effective adoption and utilization of the blockchain solution.

## **5.11. Testing and Quality Assurance**

- 5.11.1. Develop comprehensive documentation and training materials to facilitate effective adoption and utilization of the blockchain solution.

## **5.12. Deployment and Go Live**

- 5.12.1. Finalize preparations, deploy the blockchain solution, and transition to the live environment.

## **5.13. Maintenance and Support Plan**

- 5.13.1. Develop a plan for ongoing maintenance and support of the blockchain solution.

## **5.14. Per Document Tokenization Program**

- 5.14.1. The Contractor shall allow DBM to upload all the documents (maximum of 500,000 upload in one (1) year) using a blockchain as a service with Private, Public and Hybrid Accountability Ledger.

**6.0 PROVISION OF TECHNICAL SUPPORT TO DBM**

The Subscription to Immutable and Verifiable Attributes (Blockchain) for the Department of Budget and Management Action Document Releasing System (ADRS) shall include the following technical support services from the Contractor during the duration of the contract:

- 6.1. The contractor shall deploy the following technical personnel to provide technical support to the DBM:
  - 6.1.1. Project Manager
  - 6.1.2. Certified Developer
  - 6.1.3. Functional Consultant
  - 6.1.4. Support Officer
  
- 6.2. The contractor must provide twenty-four hours a day, seven days a week (24x7) technical assistance, a contact person designated by the contractor to attend to telephone call, electronic mail, and/or on-site support during the entire duration of the Project. The contact person may be required to visit DBM if deemed necessary.
  
- 6.3. The contractor warrants that the technical staff assigned are qualified to provide deliverables required to the DBM's satisfaction.

**7.0 SERVICE LEVEL AND SUBSCRIPTION AGREEMENT**

- 7.1. DBM shall maintain a Service Level Agreement (SLA) with the CONTRACTOR, with provisions for liquidated damages for their non-compliance.

Component	Description	Liquidated Damages
Delivery	The CONTRACTOR shall deliver the following Software Licenses & Platform with 1 Year Software Assurance within 30 calendar days from the issuance of Notice to Proceed (NTP) – Ready to integrate to ADRS and upload DBM actionable document.	One percent (1%) of the total contract price shall be deducted for every day of delay.
Technical Support	<p>The CONTRACTOR shall provide/render twenty-four hours a day, seven days a week (24x7) technical support service that can be delivered in the form of a telephone call, electronic mail, and/or onsite support.</p> <p>The CONTRACTOR shall resolve every problem within six (6) hours after it was reported by DBM. It shall refer to a condition wherein the</p>	One-tenth (1/10 <sup>th</sup> ) of one percent (1%) of the total contract price shall be deducted for every hour of delay.

Component	Description	Liquidated Damages
	reported problem is resolved by the CONTRACTOR to the satisfaction of the DBM. Problem and resolution shall be logged in the DBM Help Desk Facility.	

7.2. The DBM shall have the right to blacklist the CONTRACTOR after twelve (12) instances of non-compliance to Section 4.4 at any given time during the contract period.

## 8.0 QUALIFICATION OF THE CONTRACTOR

8.1. The contractor must have a proven track record in Information Technology, Software Development and Systems Integration for at least ten (10) years in the industry.

8.2. The contractor must be endorsed by the Blockchain Council of the Philippines.

8.3. The contractor must present a valid and current “Certificate of Resellership/ Distributorship” issued by the main provider of the blockchain solution.

8.4. The contractor shall have more than one (1) year of valuable professional certification for business applications per person.

## 9.0 CONFIDENTIALITY OF DATA

9.1. All project personnel of the contractor shall be required to sign a Non-Disclosure Agreement (NDA).

9.2. The contractor agrees to hold Proprietary Information in strict confidence. The contractor furthermore agrees not to reproduce, translate or disclose the Proprietary Information to 3rd parties without the prior written approval of DBM.

## 10.0 WARRANTIES OF THE CONTRACTOR

10.1. The contractor warrants that it shall conform strictly to the terms and conditions of this TOR.

10.2. The contractor warrants represent and undertake the reliability of the services and that their manpower complements are hardworking, qualified/reliable and dedicated to doing the service required to the satisfaction of the DBM. It shall employ well-behaved and honest employees with ID displayed conspicuously while working within the compound. It shall not employ DBM employees to work in any category whatsoever.

10.3. The contractor in the performance of its services shall secure, maintain at its own expense all registration, licenses or permits required by National or Local Laws and shall comply with the rules, regulations, and directives of Regulatory Authorities and Commissions. The contractor undertakes to pay all fees or changes payable to any

instrumentality of government or to any other duty constituted authority relating to the use or operation of the installation.

- 10.4. The contractor personnel shall take all necessary precautions for the safety of all persons and properties at or near their area of work and shall comply with all the standard and established safety regulations, rules and practices.
- 10.5. The contractor shall coordinate with the authorized and/or designated DBM personnel in the performance of their jobs.
- 10.6. The contractor shall be liable for loss, damage, or injury due directly or indirectly to the fault or negligence of its personnel. It shall assume full responsibility thereof and the DBM shall be specifically released from any and all liabilities arising therefrom.
- 10.7. The contractor shall neither assign, transfer, pledge, nor sub-contract any part or interest therein.

## **11.0 TERMS OF PAYMENT**

- 11.1. The CONTRACTOR shall be paid one time upon provision of licenses and platform of this Project subject to the required Final Withholding VAT (Services) of five percent (5%) and Expanded Withholding Tax of two percent (2%).
- 11.2. Payment shall be made within a reasonable time from the submission of the documentary requirements such as, but not limited to the following, based on existing accounting and auditing laws, rules and regulations:
  - i. Sales Invoicing/Billings
  - ii. Certificate of Acceptance issued by the Undersecretary of the ICT Group/Chief Information Officer
  - iii. Non-Disclosure Agreement
  - iv. Proof of Subscription
- 11.3. No advance payment shall be made as provided for in Section 88 of Presidential Decree 1445.

## **12.0 PRE-TERMINATION OF CONTRACT**

- 12.1. The contractor for this project may be pre-terminated by the DBM for any violation of the terms of the contract. In the case of pre-termination, the contractor shall be informed by the DBM thirty (30) days prior to such pre-termination.
- 12.2. In the case of pre-termination, the contractor shall be liable to additional liquidated damage equivalent to one percent (1%) of the contract price as provided by the Government Accounting Manual (GAM) and forfeiture of the Performance Security.
- 12.3. The DBM shall have the right to blacklist the contractor in case of pre-termination.