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

## SUPPLEMENTAL/BID BULLETIN (SBB) NO. 3

This SBB No. 3 dated March 11, 2025 for **Project ID No. DBM-2025-16, "Cloud Infrastructure Subscription with Support and Maintenance for the Budget and Treasury Management System (BTMS)"** is issued pursuant to Section 22.5 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184, to clarify, modify or amend items in the Bidding Documents. Accordingly, this shall form an integral part of the Bidding Documents.

<table>
<tr><th>PARTICULAR(S)/QUERY(IES)</th><th>AMENDMENT(S)/CLARIFICATION(S)</th></tr>
<tr>
<td>
<b>Annex "A"</b><br><br><b>Detailed Technical Specifications</b><br><br>xxx<br><br><b>ATTACHMENT 4<br>SCHEDULE OF PAYMENT</b><br>
<table>
<tr><th>Schedule of Payment</th><th>Amount to be paid to the Contractor</th><th>Milestones</th><th>Remarks</th></tr>
<tr><td colspan="4">xxx</td></tr>
<tr><td><b>Month 13 to 15</b></td><td>Equal Monthly Payments of 6% of Total Project Cost</td><td>• Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports</td><td>Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO.</td></tr>
<tr><td><b>Month 16 to 18</b></td><td>Equal Monthly Payments of 6% of</td><td>• Monthly Performance Reports of</td><td>Payment will be based on submission</td></tr>
</table>
</td>
<td>
<b>Annex "A"</b><br><br><b>Detailed Technical Specifications<br>(REVISED)</b><br><br>xxx<br><br><b>ATTACHMENT 4<br>SCHEDULE OF PAYMENT<br>(REVISED)</b><br>
<table>
<tr><th>Schedule of Payment</th><th>Amount to be paid to the Contractor</th><th>Milestones</th><th>Remarks</th></tr>
<tr><td colspan="4">xxx</td></tr>
<tr><td><b>Month 13 to 15</b></td><td>Equal Monthly Payments of ~~6~~ <b>8.25%</b> of Total Project Cost</td><td>• Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports</td><td>Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO.</td></tr>
<tr><td><b>Month 16 to 18</b></td><td>Equal Monthly Payments of ~~6~~</td><td>• Monthly Performance Reports of L1 and L2</td><td>Payment will be based on submission</td></tr>
</table>
</td>
</tr>
</table>

| PARTICULAR(S)/QUERY(IES) | | | | AMENDMENT(S)/CLARIFICATION(S) | | | |
|---|---|---|---|---|---|---|---|
| | Total Project Cost | L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | of Reports, deliverables, and approval thereof by the DBM OCIO. | | **8.25%** of Total Project Cost | Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 19 to 21** | Equal Monthly Payments of 6% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. | **Month 19 to 21** | Equal Monthly Payments of ~~6~~ **8.25%** of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 22 to 24** | Equal Monthly Payments of 6% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. | **Month 22 to 24** | Equal Monthly Payments of ~~6~~ **8.25%** of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| xxx | | | | xxx | | | |
| | | | | **Note:**<br>**Attached for guidance of the bidders is the Detailed Technical Specifications (Revised) which shall form part of the Bidding Documents.** | | | |

**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 March 18, 2025 right after the opening of bids.

- For guidance and information of all concerned.

**(SGD)**
**RAMON VICENTE B. ASUNCION**
*Assistant Secretary*
*Vice Chairperson, DBM-BAC*

**Annex A**

# DETAILED TECHNICAL SPECIFICATIONS (REVISED)

## 1. PROJECT TITLE

Cloud Infrastructure Subscription with Support and Maintenance for the Budget and Treasury Management System (BTMS)

## 2. OVERVIEW

The project aims to provide a *cloud environment solution* for the Department of Budget and Management (DBM) to be used for the BTMS. This solution will be critical in ensuring business continuity of the day-to-day IT operations of the Department and its Bureaus/Services/Offices (BSOs).

The BTMS is an integrated, web-based information management system that will replace the existing budget management, execution, accounting, and reporting systems initially used by the DBM and the Bureau of the Treasury (BTr) under the Department of Finance (DOF) for budget execution and accountability.

## 3. OBJECTIVES OF THE PROJECT

The project aims to:

3.1. Procure and subscribe to an *Infrastructure as a Service (IaaS) provider* for the DBM through a secure public cloud platform;

3.2. Migrate the existing BTMS cloud-hosted servers to a secure public cloud platform; and

3.3. Procure technical support services for the deployment and configuration of the cloud environment set forth by DBM for its IT environment and/or systems.

The Cloud Infrastructure Subscription with Support and Maintenance for BTMS will maintain the performance and functionality of and ensure compatibility with the existing fleet and equipment. Hence, reference to brand names is deemed authorized consistent with Section 18 of the 2016 Revised IRR of RA 9184 which provides that, "[r]eference to brand names shall not be allowed **except for items or parts that are compatible with the existing fleet of equipment of the same make and brand, and to maintain the performance, functionality and useful life of the equipment**". (emphasis supplied)

## 4. DURATION OF CONTRACT

The subscription period for this project shall run for thirty-six (36) months from the acceptance of the installation and configuration of the Cloud Infra.

## 5. SCOPE OF WORK AND DELIVERABLES

The contractor shall deliver/fulfill the following:

5.1 Subscription to Amazon Web Services (AWS) Cloud for the DBM.

5.2 Configuration and migration of the existing *BTMS Cloud* to the *AWS Cloud of DBM* for the duration of the contract.

5.3 Provision, configuration, support, and maintenance of DBM AWS services based on the BTMS sizing requirement for the environment in scope as detailed in **Attachment 1**.[1]

5.4 Migration of the specified DBM workloads to the DBM's AWS environment to be provided by the DBM during project implementation and to configure, maintain, and provide technical support in accordance with the industry's best practices.

5.5 Setup and provision of an AWS account for the DBM which shall include the following services, among others:

5.1.1. Migration of the various database and application servers
5.1.2. Migration of domain records and retention of the existing domain name of DBM
5.1.3. Configuration of and provision of technical support to the dedicated site-to-site VPN between DBM's AWS environment and DBM Data Center required resources
5.1.4. Segregation, isolation, and provision of security of the different network subnets
5.1.5. Provision of allowance for data ingress/egress
5.1.6. Provision of identities and policies for the Identity and Access Management for the AWS environment
5.1.7. Provision of technical support for the integration with existing DBM in-house applications
5.1.8. Provision of load balancing
5.1.9. Provision of an Intrusion Detection and Prevention System
5.1.10. Provision of an Endpoint Detection and Response System
5.1.11. Provision of a Firewall
5.1.12. Resource monitoring

5.5. Provision, configuration, technical support, and maintenance of technology and services consistent with the cloud services technical requirements detailed in **Attachment 2**.[2]

5.6. Provision of a dashboard interface for cloud administrators which shall provide the overall view of the size and status of the subscribed cloud environment including but not limited to performance-monitoring capabilities of the processor, memory, disk usage, and network utilization.

5.7. Provision of a Professional and Technical Support Services for the BTMS Cloud Infrastructure Subscription, as provided in **Attachment 3**.[3]

[1] *BTMS Sizing Requirements based on Rollout Strategy*

[2] *Cloud Services Technical Requirement Specifications*

[3] *Professional and Technical Support Services*

## 6. TIMELINE FOR THE PROJECT ENGAGEMENT

| Item | Description | Delivery Schedule |
|---|---|---|
| 1 | Supply, Delivery, Installation, and Configuration of Cloud Infra Subscription | Within ninety (90) calendar days upon receipt of the NTP |
| 2 | Provision of Cloud Subscription and Technical Services | Shall run for thirty-six (36) months from the installation and configuration of the Cloud Infra |
| 3 | Inception Report which includes details of the project planning framework, communications, reporting, procedural and contractual activities and weekly status reports | Within thirty (30) calendar days upon receipt of the NTP |
| 4 | Availability or assignment of technical support resources | Fifteen (15) calendar days upon receipt of the NTP |
| 5 | Provision of the proposed service credits' terms and conditions | Fifteen (15) calendar days upon receipt of the NTP |

## 7. TECHNICAL QUALIFICATION REQUIREMENTS

The Contractor must adhere to the following qualifications:

7.1. The contractor must be an authorized partner of AWS. The corresponding documentation shall be submitted during post-qualification.

7.2. The AWS account ownership and its related services shall belong to the DBM. The Access rights may be given to third party vendor/s, as deemed necessary and upon approval of the DBM, to perform any services related to the project. However, the DBM retains the authority to revoke these access rights from the root account at any time and may reassign them to another vendor as needed.

7.3. The AWS environment must be deployed in at least two (2) availability zones (AZs) in the Singapore Region and must be capable to be deployed in other ASEAN regions.

7.4. The contractor must not have access to DBM Content on their virtual machines. There must be no technical means or APIs available for the personnel of the contractor to read, copy, extract, modify, or access in any other means DBM content from a cloud virtual machine or encrypted volume attached to the virtual machine.

7.5. The contractor must have the following Certified Professionals, with each certification represented by a different individual who will handle DBM requests and activities:

7.5.1. One (1) Certified AWS Solutions Architect – Associate;
7.5.2. Two (2) Certified AWS Cloud Practitioners; and
7.5.3. One (1) Certified Cloud Security Professional (CCSP) or Certified Information Systems Security Professional (CISSP).

7.6. The contractor must provide one (1) dedicated instructor of the chosen cloud services provider to supervise the knowledge transfer and training. Accordingly, said instructor must meet the following minimum qualification requirements:

7.6.1. Must have completed at least Bachelor's Degree in Computer Engineering or Computer Science supported by College Diploma or Transcript of Record;
7.6.2. Must have at least two (2) years of relevant experience in cloud computing, information technology or ICT infrastructure management supported by Certification of Projects Completed, Certificate of Employment, or Curriculum Vitae; and
7.6.3. Must have completed at least one (1) training on cloud computing or information technology supported by Training Certificate(s)

The contractor must provide the appropriate certifications and documentary requirements of the Certified Professionals and dedicated instructor within the project implementation.

## 8. SERVICE LEVEL AGREEMENT

The Cloud Environment system shall be subject to the following Service Level Agreements (SLAs):

### 8.1. **Service Credit**

8.1.1. The service credit refers to a percentage of the total AWS cloud provider credits added to the applicable annual billing cycle of the DBM in case that the AWS cloud environment platform services fail to meet the standard monthly uptime percentage. The determination of the amount of service credit shall follow the corresponding monthly uptime percentage:

| Monthly Uptime Percentage | Service Credit Percentage |
|---|---|
| Equal to or greater than 99.0% but less than 99.5% | 10% of the total |
| Equal to or greater than 95.0% but less than 99.0% | 30% |
| Less than 95.0% | 100% |

8.1.2. The service provider shall provide monthly reports on the monthly uptime percentage subject to the validation of the DBM.

8.1.3. The service provider shall submit the proposed service credits' terms and conditions (15) calendar days upon receipt of the NTP, subject to the approval of the DBM.

8.2. **Liquidated Damages**

8.2.1. Service Level targets or Key Performance Indicators (KPIs) shall be observed monthly within the duration of the contract. Any changes thereof shall be agreed upon with the selected vendor based on standard industry measurements based on a quarterly review.

| Service Measure | Measurement | Stabilization | Steady State | Measurement Method |
|---|---|---|---|---|
| Availability of Service Desk – 24x7x365 | Monthly Average | 99.99% | 99.99% | Call Platform Uptime / Resource Access Availability |
| Speed to Answer – 30 seconds or less | Monthly Average | 80% | 99% | ACD Statistics |
| Email Response – 1 hour or less | Monthly Average | 80% | 99% | ITSM Platform |
| Self-service Response Time – 15 minutes or less | Monthly Average | 80% | 99% | ITSM Platform |
| First Contact Resolution | Monthly Average | 60% | 80% | ACD Statistics / ITSM Platform |
| Incident Assignment – 15 mins or less | Monthly Average | 70% | 90% | ITSM Platform |
| Customer Satisfaction | Monthly Average | 60% | 80% | Customer Satisfaction (CSAT) Surveys |

8.2.2. Failure to deliver the technical support services according to the above service level targets and requirements set by the DBM shall be subject to liquidated damages equivalent to the following, pursuant to Section 68 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184:

| Service Measure | Liquidated damages |
|---|---|
| Availability of Service Desk – 24x7x365 | 1/10th of 1% of the monthly equivalent of the quarterly payment shall be imposed per day of delay |

| | |
|---|---|
| Speed to Answer – 30 seconds or less | 1/10th of 1% of the monthly equivalent of the quarterly payment shall be imposed per 30 seconds of delay |
| Email Response – 1 hour or less | 1/10th of 1% of the monthly equivalent of the quarterly payment shall be imposed per day of delay |
| Self-service Response Time – 15 minutes or less | 1/10th of 1% of the monthly equivalent of the quarterly payment shall be imposed per minute of delay |
| First Contact Resolution | 1/10th of 1% of the monthly equivalent of the quarterly payment shall be imposed per day of delay |
| Incident Assignment – 15 mins or less | 1/10th of 1% of the monthly equivalent of the quarterly payment shall be imposed per minute of delay |
| Customer Satisfaction | 1/10th of 1% of the monthly equivalent of the quarterly payment shall be imposed per day of delay |

## 9. OBLIGATIONS OF THE CONTRACTOR

9.1. The contractor shall strictly conform with the terms and conditions stipulated in the Detailed Technical Specifications and report directly to the Office of the Functional Group Head of the ICT Group / Chief Information Officer (OCIO) of DBM.

9.2. The contractor must provide incident management with respect to the DBM's Operational Standards.

9.3. The contractor must provide post-implementation technical support to and observe regular maintenance of the DBM's Cloud environment to minimize unplanned interruptions to services by way of regular reviews.

9.4. The contractor shall inform the DBM in writing of any circumstances that may cause delays in execution and/or fulfillment of the contract.

9.5. The contractor shall inform the DBM in writing of any possible need for extension of the duration of the services and its corresponding commercial implications, subject to applicable procurement, budgeting, accounting, and auditing laws rules and regulations

9.6. As part of project management, the contractor shall provide a timeline of the services to be performed, in accordance with the planned activities for the project.

9.7. The contractor shall provide a signoff document[1] to the DBM once certain activities and/or scopes of the contract has been completed by the supplier.

9.8. The cloud service provider (CSP), as the core component of this solution, should adhere to the Service Level Agreement and should be subject to the CSP Shared

[1] *Shall serve as basis for the issuance of partial and final certificate of acceptance by the DBM.*

Responsibility Model. The shared responsibility must at minimum include the following particulars:

<table>
<tr><th>Responsible</th><th colspan="4">Particulars</th></tr>
<tr><td rowspan="4"><b>Customer Responsibility for Security 'IN' the CLOUD</b></td><td colspan="4">Customer Data</td></tr>
<tr><td colspan="4">Platform, Applications, Identity &amp; Access Management</td></tr>
<tr><td colspan="4">Operating System, Network &amp; Firewall Configuration</td></tr>
<tr><td>Client-Side Data Encryption &amp; Data Integrity Authentication</td><td>Server-side Encryption (File System and/or Data)</td><td colspan="2">Networking Traffic Protection (Encryption, Integrity, Identity)</td></tr>
<tr><td rowspan="4"><b>CSP Responsibility for security 'OF' the CLOUD</b></td><td colspan="4">Software</td></tr>
<tr><td>Compute</td><td>Storage</td><td>Database</td><td>Networking</td></tr>
<tr><td colspan="4">Hardware/AWS Global Infrastructure</td></tr>
<tr><td>Regions</td><td>Availability</td><td colspan="2">Edge Locations</td></tr>
</table>

9.9. Assignment of a Single Point of Contact (SPOC) within the Contractor’s team who will serve as the primary point of contact for any concerns and/or inquiries on the execution of the professional and technical support services.

9.10. Maintenance of a satisfactory level of performance throughout the term of the contract based on the prescribed set of performance criteria, which include, but not limited to the: (i) quality of service delivered; (ii) ability to meet defined Service Levels/Key Performance Indicators (KPIs); (iii) ability to contract administration and management; and (iv) compliance with the required regular performance reports.

## 10. OBLIGATIONS OF THE PROCURING ENTITY

10.1. The DBM shall provide the necessary resources for the professional and technical support personnel to be deployed for the project, which shall include internet connection, utilities, office access, repository access, admin access, and database access as may be necessary to perform the deliverables of the project.

10.2. The DBM shall be responsible for regular activities involving the use of the agile methodology approach such as scrum, daily huddles, and sprint planning to ensure timely and quality accomplishment of the project deliverables.

10.3. The DBM shall orient the contractor on the DBM’s policies, procedures, and work assignment.

10.4. The DBM shall grant the necessary access roles and levels to the contractor as part of the fulfillment of the defined scope of work to be provided by the contractor.

10.5. The DBM shall assign its SPOC which shall act as the primary point of contact to address any issues related to the scope of work during the implementation of the project.

10.6. DBM may opt to extend the engagement, as necessary, subject to RA No. 9184 and its revised IRR, which shall be done through a formal request to be issued at least thirty (30) calendar days prior to end of the contract.

10.7. The AWS environment to be used and configured by the contractor's team shall be under the ownership model of a technical support service provision.

10.8. The DBM will be responsible for actions of their systems specifically for the applications and databases used and utilized within their environment, and by its users, respectively.

10.9. DBM will be responsible for the development and/or troubleshooting of the components outside the contractor's scope of work.

10.10. Any incidents that may happen during the duration of the contract shall be resolved by the operational team of DBM with support from the contractor in cases where the incident is within the contractor's scope of work.

10.11. The DBM shall be responsible for all license subscriptions outside the scope of work that will be used in this engagement such as, but not limited to, application-specific licenses.

## 11. DATA SOVEREIGNTY

11.1. DBM subject to conditions prescribed by the Law of the Republic of the Philippines with regards to data residency and sovereignty laws, retains control and ownership of all data stored or processed during the subscription period.

11.2. All DBM Data stored in the contractor's system shall be the sole property of the DBM. This data can be retrieved anytime upon request of the DBM and has the sole right and authority to copy, move, delete, or transfer it to other locations.

11.3. Except as otherwise permitted under Philippine law, no data shall be subject to foreign laws, or be accessible to other countries, regardless of the system used, the nationality of the contractor, or the data's place of storage, processing, or transmission. No rights appurtenant to such data shall be deemed transferred or assigned by virtue of the storage, processing, or transmission thereof by the contractor.

11.4. The contractor must agree and ensure that the data stored in the proposed location will remain within it and will not be transferred without the knowledge and permission of the DBM.

## 12. CONFIDENTIALITY OF DATA

12.1. The contractor shall be required to sign a Non-Disclosure Agreement (NDA) to be provided by the DBM and signed by the contractor within ninety (90) calendar days upon receipt of the Notice to Proceed.

12.2. The DBM Enterprise Network System, its components, parts, and all products, products samples and specifications, data, ideas, technology, and technical/non-technical materials, all or any which may be derived from any of the foregoing are considered strictly confidential.

12.3. The contractor agrees to hold all the foregoing information in strict confidence. The contractor further agrees not to reproduce or disclose any confidential information to third parties without prior written approval of the DBM.

## 13. TERMS OF PAYMENT

13.1. Payment shall be made in accordance with the schedule reflected in **Attachment 4** (Schedule of Payment), subject to the satisfactory accomplishment of the project deliverables and complete submission of the following documentary requirements:

13.1.1. **Document for the initial payment:**

13.1.1.1. Non-Disclosure Agreement (NDA);

13.1.1.2. Valid and updated Tax Clearance Certificate;

13.1.1.3. Sales Invoice / Billing Statement; and

13.1.1.4. Partial Certificate of Acceptance issued by the Undersecretary for Information and Communications Technology (ICT) Group.

13.1.2. **Document for final payment:**

13.1.2.1. Valid and updated Tax Clearance Certificate;

13.1.2.2. Non-Disclosure Agreement (NDA);

13.1.2.3. Sales Invoice / Billing Statement; and

13.1.2.4. Certificate of Acceptance issued by the Undersecretary for Information and Communications Technology (ICT) Group.

## ATTACHMENT 1
## BTMS SIZING REQUIREMENTS BASED ON ROLLOUT STRATEGY

| **Particular** | **Description** | | |
|---|---|---|---|
| **Year** | **1** | **2** | **3** |
| **Host Type** | **App Server (Production)** | | |
| Number of VMs | 2 | 7 | 8 |
| Total vCPU per Server | 64 | 64 | 64 |
| Total vRAM per Server | 256 GiB | 256 GiB | 256 GiB |
| Total Storage per Server | 300 GiB | 300 GiB | 300 GiB |
| **Host Type** | **App Server (Non-Production)** | | |
| Number of VMs | 4 | 4 | 4 |
| Total vCPU per Server | 64 | 64 | 64 |
| Total vRAM per Server | 256 GiB | 256 GiB | 256 GiB |
| Total Storage per Server | 300 GiB | 200 GiB | 200 GiB |
| **Host Type** | **Database Server (Production)** | | |
| Number of RDS | 1 | 1 | 1 |
| Total vCPU per Server | 64 | 64 | 64 |
| Total vRAM per Server | 256 GiB | 256 GiB | 256 GiB |
| Total Storage per Server | 1500 GiB | 1500 GiB | 1500 GiB |
| Backup Storage | 2000 GiB | 2000 GiB | 2000 GiB |
| **Host Type** | **Database Server (Non-Production)** | | |
| Number of RDS | 1 | 1 | 1 |
| Total vCPU per Server | 48 | 48 | 48 |
| Total vRAM per Server | 192 GiB | 192 GiB | 192 GiB |
| Total Storage per Server | 750 GiB | 750 GiB | 750 GiB |

| | | | |
|---|---|---|---|
| Backup Storage | 1500 GiB | 1500 GiB | 1500 GiB |
| **Object Storage** | 750 GiB / month storage and transfer | | |
| **IP Addresses** | Public and Private (with capability to be static) | | |
| **Security** | ● Identity Access Management<br>● Network Firewall<br>● Threat Detection and Monitoring<br>● Intrusion Detection and Prevention System (IDS/IPS)<br>● Web Application Firewall | | |
| **Network** | ● 4 site-to-site VPN connections<br>● 5TB of Network Ingress/Egress per month<br>● Load Balancer of at a minimum of 500 Megabits per second (Mbps) bandwidth 24x7.<br>● Managed NAT service deployed in multiple AZs | | |
| **Operating System** | Windows Server 2022 | | |
| **Database Server** | MS-SQL Server Enterprise in High Availability (prod)<br>MS-SQL Server Standard (non-prod) | | |
| **DNS Server** | Must retain the existing domain name used by the DBM. | | |
| **Region**[1] | Production Environment/Instances – Must run in the Singapore region in at least two (2) AZs<br>Development Environment/Instances – Must run in the Singapore region in at least one (1) AZ | | |
| **Credits** | The contractor must provide Php 150,000,000.00 worth of cloud provider credits to the DBM for the operation of the infrastructure covering thirty-six (36) months or three (3) years.<br>The DBM may use the said credits as they see fit until the same are fully consumed.<br>The contractor must submit monthly utilization reports to DBM. | | |

***Note****: Quantities stated above are indicative only and may increase or decrease based on actual requirements during contract implementation. The contractor shall inform DBM when*

[1] *Consistent with DICT Department Circular 010 dated 02 June 2020*

*80% of the budgeted credits have been consumed. Accordingly, additional procurement activities may be conducted in the event that the total credit utilization exceeds the forecasted baselines, as necessary and in accordance with applicable procurement guidelines, laws, rules, and regulations.*

# ATTACHMENT 2
# CLOUD SERVICES TECHNICAL REQUIREMENT SPECIFICATIONS

## 1. GENERAL SECURITY REQUIREMENT

1.1 The proposed cloud solution should meet international security standards and should comply with all relevant Philippine laws, rules and regulations.

1.2 The proposed cloud solution must provide an isolated network virtualization to reduce the risk of attack exploits on the cloud hypervisor.

1.3 The proposed cloud solution must have a native network firewall to secure the public-facing web servers.

1.4 The proposed cloud solution must enable least-privilege access to reduce the risk of overly permissioned users or applications.

1.5 The proposed cloud solution should be able to identify, monitor, and remediate threats, issues, and inconsistencies across all resources in the Amazon Web Services (AWS) subscribed environment.

1.6 The proposed solution must provide the appropriate licenses with Extended Detection and Response (XDR) capabilities for both the integrated on-premises servers/systems and the cloud infrastructure resources.

1.7 The proposed solution must be able to provide a web-based single management console for both on-premises and cloud servers.

1.8 The proposed solution must provide a layered defense against advanced attacks and provide protection against known and unknown vulnerabilities in the web, enterprise applications, and operating systems.

1.9 The proposed solution must be able to support web reputation to prevent access to malicious websites.

1.10 The proposed solution must be able to support Docker hosts and containers running on Windows and different Linux distributions.

1.11 The proposed solution must be able to support legacy operating systems.

1.12 The solution must be able to support integrations to an on-premise datacenter, hybrid datacenter, or other cloud providers such as Google Cloud and Microsoft Azure.

1.13 The solution must monitor inter-VM traffic and workload instances.

1.14 The proposed solution must be able to protect a wide range of platforms: Windows, different Linux distributions, Solaris, HP-UX, AIX, VMware, Citrix, Hyper-V, Amazon EC2, Azure VM.

1.15 The proposed solution must be able to provide multiple layers of security within a single agent such as:

1.15.1 Host-Based Intrusion Prevention
1.15.2 File-Integrity Monitoring
1.15.3 Behavioral Analysis
1.15.4 Vulnerability Scanning

1.15.5 Host-based Firewall
1.15.6 Application Control
1.15.7 Log Inspection
1.15.8 Anti-malware
1.15.9 Web Reputation
1.15.10 Sandboxing Analysis

1.16 The proposed solution must have a predictive machine learning capability to protect against unknown malwares.

1.17 The proposed solution must have behavioral monitoring to protect against malicious scripts and applications.

1.18 The proposed solution must have the capability to receive hash code from the virtual analyzer to block unknown malwares.

## 2. INTRUSION DETECTION AND PREVENTION SYSTEM

2.1 The proposed solution must be able to provide Host Intrusion Prevention System (HIPS)/ Host Intrusion Detection System (HIDS) features.

2.2 The proposed Solution must be able to provide HIPS/HIDS for containers.

2.3 The proposed solution must be able to provide a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, contents that signal an attack, and policy violations.

2.4 The proposed solution must be able to operate in detection or prevention mode to protect operating systems and enterprise applications against vulnerabilities.

2.5 The proposed solution must be able to provide protection against known and zero-day attacks.

2.6 The proposed solution must be able to push protection policies without the need for a system reboot.

2.7 The proposed solution must be able to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing a malicious code.

## 3. VIRTUAL PATCHING

3.1 The proposed solution must be able to provide a virtual patching that shields and protects vulnerable systems while waiting for a permanent security patch.

3.2 The proposed solution must be able to provide a virtual patch within an hour and push out the protection to thousands of VMs within minutes without disrupting normal operations.

3.3 The proposed solution must have vulnerability rules to shield known vulnerabilities from an unlimited number of exploits and automatically shield newly-discovered vulnerabilities within an hour.

3.4 The proposed solution must have the intelligence to provide recommended virtual patching rules to protect the Operating Systems (OSes) and applications.

## 4. INTEGRITY MONITORING

4.1 The proposed solution must be able to monitor critical OS and application files such as directories, registry keys and values to detect and report malicious and unexpected changes in real-time.

4.2 The proposed solution must be able to provide alerts when unauthorized changes occur.

4.3 The proposed solution must be able to provide recommendation scans and baseline scanning.

## 5. HOST-BASED FIREWALL

5.1 The proposed solution must be able to provide an enterprise-grade, bi-directional stateful firewall providing a centralized management of firewall policy including the predefined templates such as:

5.1.1 Virtual machine isolation;
5.1.2 Fine-grained filtering of Internet Protocol (IP) and Media Access Control (MAC) addresses and ports;
5.1.3 Coverage of all IP-based protocols and all frame type;
5.1.4 Prevention of denial of service (DoS) attack;
5.1.5 Design policies per network interface; and
5.1.6 Detection of reconnaissance scans.

## 6. APPLICATION CONTROL MODULES

6.1 The proposed solution must be able to monitor changes made to the server compared to baseline software.

6.2 The proposed solution must be able to allow or block software and optionally lock down the server from an unauthorized change.

6.3 The proposed solution must be able to provide a maintenance mode that will allow installation of software and changes in the OS.

6.4 The proposed solution must be able to provide alerts in the console when there are unauthorized scripts running in the application.

## 7. LOG INSPECTION

7.1 The proposed solution must be able to provide the capability to inspect logs and events generated by OSes and applications.

7.2 The proposed solution must be able to automatically recommend and unassign log inspection rules that are not required.

7.3 The proposed solution must be able to provide a predefined template for OSes and enterprise applications to avoid manual creation of the rules.

7.4 The proposed solution must be able to create a customized rule to support custom applications.

7.5 The proposed solution must use a single console when managing and viewing alerts of VMs and Containers.

## 8. SECURITY MANAGEMENT CONSOLE

8.1 The proposed solution shall be able to integrate into a Security Information and Event Management (SIEM) and Active Directory.

8.2 The proposed solution shall be able to manage both on-premises and cloud agents.

8.3 The proposed solution shall have the capability to display multiple information in the dashboard.

8.4 The proposed solution shall have a web-based management system for administrators.

8.5 The proposed solution shall be able to support Windows or Linux Management Server.

8.6 The proposed solution shall be able to provide alerts on the main menu to view notifications concerning system or security events.

8.7 The proposed solution shall be able to provide firewall events to view activities on the systems such as dropped or logged packets.

## 9. CLOUD SECURITY MANAGEMENT

9.1 The proposed solution must be able to install a security agent through user data and deployment script.

9.2 The proposed solution must be able to apply a security policy automatically after installing the agent.

9.3 The proposed solution must be able to integrate the security agent into the image and WorkSpaces bundle.

9.4 The proposed solution must be able to support auto-scaling to automatically protect new instances.

## 10. INTEGRATION

10.1 Provide remote management to the cloud-hosted servers using native functionality within the cloud contractor.

10.2 Ensure that in-house applications such as the BTMS are operational upon the application migration.

## 11. TRAINING

11.1 The contractor must provide AWS Solutions Architect – Associate and Cloud Technical Essentials Learning Path for fifteen (15) nominated technical personnel resources.

11.2 The contractor must provide access to an online, self-paced, training platform for cloud enablement, including cloud development, architecting, operations, and security.

11.3 The platform must be the official online learning platform of AWS.

11.4 The hands-on training shall be conducted at no additional cost to the DBM.

11.5 The learning courses must be certified as official by AWS.

11.6 The learning courses must be delivered synchronously and face-to-face with an AWS' affiliated training partner.

## 12. ENTERPRISE INFRASTRUCTURE AUTOMATION PLATFORM

12.1 Must be able to manage physical / VMs, and network / security devices regardless of where they are deployed on-premise or virtualized, in the cloud.

12.2 Must be able to connect to central repositories such as Github, Bitbucket, etc.

12.3 Must have the capability to use Role-based access control.

12.4 Can be deployed in a VM or container using Windows/Linux.

12.5 Must be able to automate IT infrastructure devices without the use of agents

12.6 Must be able to connect to IT Infrastructure devices through the use of industry standard protocols such as Secure Socket Shell (SSH), Windows Remote Management (WinRM), Network Configuration Protocol (NETCONF), and Representational State Transfer Application Programming Interface (REST API).

12.7 Must be able to integrate with common IT tools that enable workflows, ticketing, identity management, etc.

12.8 Must automate manual tasks by describing the desired ideal state for the IT Infrastructure device.

12.9 Must be able to abort the execution of automation tasks if they have already been carried out against the IT infrastructure devices.

12.10 Must be able to integrate with a solution that provides a dashboard that shows information on potential issues and solutions for the Automation Platform, overview of the state of the automation operations, and a view on how much time has been saved using automation.

12.11 Must be able to provide a self-service capability that would abstract complexity from non-users.

12.12 Must be able to provide a job scheduling capability that would allow the administrators to schedule automation tasks, as well as divide the job into batches.

## ATTACHMENT 3
## PROFESSIONAL AND TECHNICAL SUPPORT SERVICES REQUIREMENT

### 1. PROVISION, MIGRATION AND CONFIGURATION FOR DBM CLOUD HOSTING

1.1. The scope of the deployment and configuration of the AWS environment shall be the following:

| Specification | Description |
|---|---|
| Provision, Migration and Configuration for DBM Cloud Hosting | To migrate the specified DBM workloads on the provided Cloud Environment Subscription and configure the same according to the following:<br>• Setup, provision, and configuration of Cloud Environment account for the DBM<br>• Transfer of Cloud Subscription from the BTMS Vendor<br>• Migration of domain records and retention of existing domain name of the DBM<br>• Allowance for data ingress/egress<br>• Provision of identities and policies for Identity and Access Management<br>• Provision of load balancing<br>• Provision of an Intrusion Prevention System<br>• Provision of an Endpoint Detection and Response System<br>• Provision of a Firewall<br>• Conduct of Resource monitoring |

1.2. The estimated schedule of deployment for this engagement should be within (90) calendar days upon receipt of the NTP and will be delivered in a mutually agreed manner.

1.3. The contractor shall submit a Project Management Plan based on approval of the Inception Reports, which shall provide a framework for project planning, communications, reporting, procedural and contractual activities. Weekly status reports shall be submitted accordingly.

1.4. The contractor must submit the following requirements:

1.4.1. Project Charter at a minimum that shall show the initial project plan, schedules, and communications plans

1.4.2. Migration Plan Document that shall include but not limited to the following:

1.4.2.1. Virtual Machines Assessment

1.4.2.2. Migration Schedule

1.4.2.3. Recommendation Plans

1.4.3. Any other requirements as deemed necessary for the operation of the BTMS application, as instructed by the DBM-Office of the Chief Information Officer

## 2. TECHNICAL SUPPORT SERVICES

The contractor shall provide the following:

2.1. Deployment of personnel for the Project should either be on-site or off-site, as may be required by the DBM. All Level 1 (L1) and Level 2 (L2) personnel shall provide sixteen hours for three hundred sixty-five days (16x365) support coverage.

2.2. Equipment, such as laptops and other peripherals, should be provided by the contractor.

2.3. Availability or assignment of technical support resources should be within fifteen (15) calendar days after the receipt of the NTP.

2.4. Replacement of personnel due to resignation or separation from the firm should be done immediately so as not to cause any disruptions in the project implementation.

2.5. The Technical Support Services shall provide a tool to track, correlate, and provide reporting and dashboard capabilities for all issues, concerns, and/or incidents.

2.6. The Technical Support Services shall coordinate and/or collaborate with any future process enhancements which may include centralizing the L1 services.

2.7. The Technical Support Services must provide a support team consisting at a minimum of the following roles:

2.7.1. Service Delivery Manager
2.7.2. Technical Lead
2.7.3. Change Management Specialist
2.7.4. Technical Document Analyst

2.8. The following **IT Service Management (ITSM)** shall include the following subset of Services:

2.8.1. Incident Management
2.8.2. Service Request Management
2.8.3. Problem Management
2.8.4. Knowledge Management
2.8.5. Asset Inventory Management

2.9. **L1 Service Desk** shall include the subset of the following services:

2.9.1. L1 Support coverage of 16x7

2.9.2. Provide at least three (3) Full Time Equivalents (FTEs) available during the support coverage.

2.9.3. To be able to service calls, a 24x7 Customer Portal, dedicated support phone number, and support email shall be provided to enable customers to log services calls through these three (3) methods.

2.9.4. Triage and resolution of incidents and service requests for in-scope services.

2.9.5. Remote User Support.

2.9.6. Provide Level 1 BTMS Application support.

2.9.7. Management and logging of all in-scope service calls until resolution, including evaluating their urgency, impact and priority.

2.9.8. Responding to and invoking DBM's Incident Response process as required.

2.9.9. Acting as the single point of contact to receive updates on active tickets.

2.9.10. Managing escalations as required.

2.9.11. Conduct of proactive performance monitoring

2.9.12. Conduct of service availability monitoring

2.9.13. Preparation of call handling workflow.

2.9.14. Facilitation of ticket handling and reassignment.

2.9.15. Liaising with AWS for any related concerns or incidents

2.9.16. Managing of escalations as required.

2.10. **Level 2 Support** shall include the subset of the following services:

2.10.1. Provision of L2 Support coverage of 16x7 (7am to 11pm)

2.10.2. Provision of at least seven (7) Full Time Equivalents (FTEs) available during the support coverage consisting of the following roles:

2.10.2.1. One (1) FTEs L2 Database Administrators

2.10.2.2. One (1) FTEs L2 Systems Administrators

2.10.2.3. Two (2) FTEs L2 Application Support

2.10.2.4. One (1) FTEs L2 Cloud Administrators

2.10.2.5. One (1) FTEs L2 Security Administrators

2.10.2.6. One (1) FTEs L2 Senior Cloud Administrators

2.10.3. Perform BTMS application troubleshooting and coordinate with the BTMS vendor to resolve issue/s and determine root cause.

2.10.4. Performance of cloud, platform, systems, and database administration control functions to support existing systems and plan new systems and planning of required changes in systems platform and/or database due to business growth and project implementation.

2.10.5. Maintenance of systems platform, applications, and databases to meet performance standards, maximize efficiency, and minimize outages, as necessary.

2.10.6. Maintenance, updating, and implementation of cloud infrastructure, platform, systems application, and database archive processes and procedures to recover from an outage or corruption based on the DBM's business requirements.

2.10.7. Troubleshooting and conduct of diagnostic activities (e.g., system logs, and monitoring tools) to investigate and resolve complex or critical tickets.

2.10.8. Performance of in-depth analysis, troubleshooting, and root cause analysis of complex incidents and use of system logs and monitoring tools for detailed diagnostics.

2.10.9. Regular monitoring of application systems and database performance, utilization, and efficiency identifying potential issues, and recommending preventive actions before they become incidents causing harm or damage

2.10.10. Monitoring of cloud VMs and related cloud resources including, but not limited to, availability, utilization, and security of the environment.

2.10.11. Performance of upgrades, patches, and bug fix(es) on cloud resources.

2.10.12. Submission of activity status report with recommendations covering at least the following:

2.10.12.1. Orphaned resource identification and cleanup

2.10.12.2. Credential audit

2.10.12.3. Overall system health based on CPU, memory, disk usage, and network performance

2.10.13. Fulfillment of service requests following the proper change management procedures

2.10.14. Regular updating and patching of OSes to ensure security and performance.

2.10.15. OS tuning for optimal performance based on workload and resource availability.

2.10.16. Ensure that OSes comply with the organizational and industry security standards required and provided by the DBM.

2.11. The Technical Support Services must include the following reports to support the Continuous Improvement (CI) roadmap for Technical Support Services.

| | **Item** | **Description** |
|---|---|---|
| **Update the following:** | | |
| 1 | Support Operational Manual | Contains support scope, RACI, processes, standard operating procedures and escalation details |
| 2 | Process Templates | Process workflow diagram for support workshop and transition |
| 3 | Support Frequently Asked Questions (FAQ) | FAQs and issues raised about the platform that will guide support team to improve handling time |
| 4 | System Catalog | Documentation of the technical details of the platform including server, services installed, and technical diagram. |
| 5 | Support Signoff | Documents service validation and signoff |
| The initial documentation stated above must be provided by the BTMS application vendor as part of their transition to the contractor. Thereafter, the contractor will take care of further updating for the continual improvement of the same. | | |
| 6 | Support Operating Report | As part of monthly monitoring and reporting, the contractor will submit a summary of issues handled, highlights, and SLA Compliance for each month of the subscription period. |

2.12. The Technical Support Services shall be subject to the following services commitment:

| Severity | Response Time | Resolution Time |
|---|---|---|
| **Severity 1**<br>Total failure of Service. The function/ system is rendered unusable for a majority (70% to 100%) of the VM services of the production environment | 30 minutes | 2 hours<br>(Upon Qualification) |
| **Severity 2**<br>Performance degradations. Some system capabilities are not working. The function/system is rendered unusable for a subset (30% to 70%) of the VM services in the production environment. | 1 hour | 4 hours<br>(Upon Qualification) |
| **Severity 3**<br>Service is available, but selected devices/users are affected. | 2 hours | 24 hours<br>(Upon Qualification) |
| **Severity 4**<br>A general usage question, reporting of a documentation error, or recommendation for product enhancement or modification. Operations continue to function\by using a procedural workaround, among others. | 4 hours | 48 hours<br>(Upon Qualification) |

Failure to comply to the above service commitment shall be subject to liquidated damages pursuant to Section 8.2.2 of the Detailed Technical Specifications

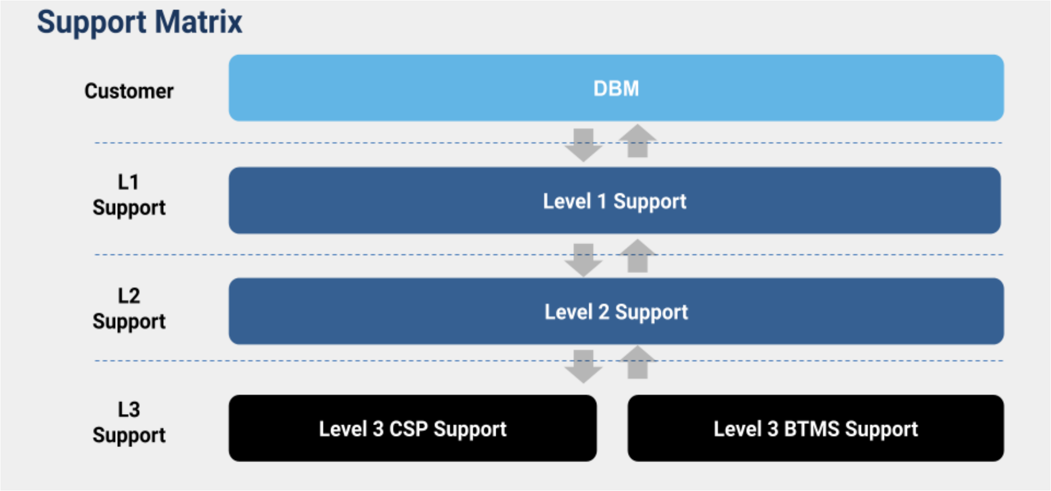
## 2.8 SUPPORT MATRIX

2.8.1 The support services and corresponding roles and responsibilities are assigned as follows:

| TASK | CONTRACTOR | DBM | BTMS APP VENDOR | CSP |
|---|---|---|---|---|
| Catch and Dispatch | R, A | | | |
| Application Runbook Support | R, A | | | |
| Creation of Runbook Support Templates | C, I | | R, A | |
| Ticket Creation/Follow Up/Closure | | R, A | | |
| Infrastructure Service Requests | R, A | C, I | | C |
| Infrastructure Incident Management | R, A | C, I | | C |
| Infrastructure Proactive Recommendations | R, A | C, I | | C |
| Operating System Level Patching | R, A | C, I | C, I | |
| Creation of Application Level Patches | I | C | R, A | |
| Installation of Application Level Patches | R, A | C, I | C, I | |
| Application System Administration | | R, A | C | |
| Cloud Service Provider (CSP) Responsibility for management 'of' the CLOUD | | C, I | | R, A |

**Legend: R** – Responsible, **A** – Accountable, **C** – Consulted, **I** – Informed

2.8.2 The support matrix for the selected supplier of the DBM shall be the following:



## ATTACHMENT 4
## SCHEDULE OF PAYMENT
## (REVISED)

On an annual basis, the schedule of payment shall be based on the following milestones:

| **Schedule of Payment** | **Amount to be paid to the Contractor** | **Milestones** | **Remarks** |
|---|---|---|---|
| **Month 1 to 3** | 11% of total project cost | • Project Plan Documents and Kick-Off Meeting<br>• Discussion of Project Activities,<br>• Inception Report<br>• Project Charter<br>• Project Management Plan<br>• Change Management Plan<br>• Migration Overview and System Design and Architecture<br>• High-Level Project Gantt Chart<br>• Requirements Validation & Sign-Off<br>• Risk Management Plan<br>• Final Agreed Project Gantt Chart | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
|  | Equal Monthly Payments of 4% of | • Monthly Performance Reports of L1 and L2 | Payment will be based on submission |

| | | | |
|---|---|---|---|
| | Total Project Cost | Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 4 to 6** | Equal Monthly Payments of 6% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 7 to 9** | Equal Monthly Payments of 6% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 10 to 12** | Equal Monthly Payments of 6% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 13 to 15** | Equal Monthly Payments of 8.25% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 16 to 18** | Equal Monthly Payments of 8.25% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 19 to 21** | Equal Monthly Payments of 8.25% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 22 to 24** | Equal Monthly Payments of 8.25% of Total Project | • Monthly Performance Reports of L1 and L2 Key Performance | Payment will be based on submission of Reports, |

| | | | |
|---|---|---|---|
| | Cost | Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | deliverables, and approval thereof by the DBM OCIO. |
| **Month 25 to 27** | Equal Monthly Payments of 6% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 28 to 30** | Equal Monthly Payments of 6% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 31 to 33** | Equal Monthly Payments of 6% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| **Month 34 to 36** | Equal Monthly Payments of 4% of Total Project Cost | • Monthly Performance Reports of L1 and L2 Key Performance Indicators (KPIs)<br>• Monthly AWS Cost Utilization Reports | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |
| | 12% of total project cost | Turnover of all relevant documentation such as Cloud System Architecture, System Accounts, Knowledge Base, and other relevant project documentation. | Payment will be based on submission of Reports, deliverables, and approval thereof by the DBM OCIO. |