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

SUPPLEMENTAL/BID BULLETIN (SBB) NO. 2

This SBB No. 2 dated November 28, 2023 for **Project ID No. DBM-2024-06, "Managed Services for Cybersecurity Posture Assessment for the Department of Budget and Management (DBM),"** 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.

PARTICULARS	AMENDMENTS
Section IV. Terms of Reference	**Section IV. Terms of Reference (REVISED)**
xxx	xxx
4.0 SCOPE OF WORK	4.0 SCOPE OF WORK
xxx	xxx
4.1 The Consultant must be able to provide the assessment One (1)-time IT Security Posture Assessment of the DBM using the eighteen (18) Computer Information System (CIS) Critical Security Controls framework below, to establish the IT security posture baseline of the DBM:	4.1 The Consultant must be able to provide the assessment One (1)-time IT Security Posture Assessment of the DBM using the eighteen (18) ~~Computer Information System~~ **CENTER FOR INTERNET SECURITY** (CIS) Critical Security Controls framework below, to establish the IT security posture baseline of the DBM:
xxx	xxx

4.1.19. Source Code Review.	4.1.19. Source Code Review **OF THE FOLLOWING**~~.~~;
	4.1.19.1 TYPESCRIPT;
	4.1.19.2 JAVA;
	4.1.19.3 JAVASCRIPT;
	4.1.19.4 PHYTON;
	4.1.19.5 PHP;
	4.1.19.6 .NET; AND
	4.1.19.7 POWERBUILDER
	THE DEVELOPMENT PLATFORMS INCLUDE APPIAN, OUTSYSTEMS

<table>
<tr>
<td>

xxx

8.0 TERMS OF PAYMENT

xxx

<table>
<tr><th>Project Activity/ Detailed Activities</th><th>Deliverables</th><th>Amount to be paid (% of Total Project Cost)</th><th>Date of Submission of Deliverables</th></tr>
<tr><td colspan="4">xxx</td></tr>
<tr><td>Third Tranche
xxx</td><td>Full Implementation Plan for Project Completion
● Risk Management and Business Continuity Plan
xxx</td><td>xxx</td><td>xxx</td></tr>
</table>

</td>
<td>

AND APPLICATION PROGRAMMING INTERFACE CONNECT.

xxx

8.0 TERMS OF PAYMENT

xxx

<table>
<tr><th>Project Activity/ Detailed Activities</th><th>Deliverables</th><th>Amount to be paid (% of Total Project Cost)</th><th>Date of Submission of Deliverables</th></tr>
<tr><td colspan="4">xxx</td></tr>
<tr><td>Third Tranche
xxx</td><td>Full Implementation Plan for Project Completion
● Risk Management ~~and~~ **PLAN WITH RESULTS OF THE POSTURES ASSESSMENT WHICH WILL PROVIDE INFORMATION ON THE GAPS, VULNERABILITIES, AND TECHNICAL RISKS RELATED TO THE CYBERSECURITY STANCE OF THE DBM. THESE RISKS WILL UNDERGO THE RISK MANAGEMENT PROCESS COVERING THE FOLLOWING PHASES**</td><td>xxx</td><td>xxx</td></tr>
</table>

</td>
</tr>
</table>

			(AMONG OTHERS): - **RISK IDENTIFICATION (INCLUSIVE OF ESTABLISHING CONTEXT AND RISK CRITERIA FOR CYBERSECURITY RISKS)** - **RISK ANALYSIS** - **RISK EVALUATION** - **RISK TREATMENT** ● Business Continuity Plan **WHICH INCLUDES RECOMMENDATIONS ON THE FOLLOWING:** - **BUSINESS CONTINUITY STRATEGY (INCLUSIVE OF BUSINESS FUNCTION RECOVERY PRIORITIES, RELOCATION STRATEGY, IF NEEDED, RECOVERY PLAN PHASES, VITAL RECORDS BACKUP, RESTORATION OF PHYSICA**		

			L DOCUMENTS WHEN WARRANTED, ON-LINE ACCESS AND INTERDEPENDENCIES ON SYSTEMS) - RECOVERY TEAMS (INCLUSIVE OF RECOVERY TEAM DESCRIPTIONS, TEAM ASSIGNMENTS, PERSONNEL NOTIFICATION, TEAM CONTACTS AND RESPONSIBILITIES) - RECOVERY PROCEDURES (INCLUSIVE OF RECOVERY ACTIVITIES AND TASKS FROM CRITICAL CYBERSECURITY INCIDENT OCCURRENCE TO PLAN ACTIVATION TO ALTERNATE SITE OPERATIONS TO TRANSITION TO PRIMARY		

	OPERATIONS) xxx		

TPF 8. Activity (Work) Schedule	**TPF 8. Activity (Work) Schedule (REVISED)**

	Month											
	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th
Activity (Work) **to be provided by the Bidder, this should be consistent with the Terms of Reference (TOR)*												
________________												

	Month											
	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th
Activity (Work) ~~**to be provided by the Bidder, this should be consistent with the Terms of Reference (TOR)*~~												
FIRST TRANCHE												
SECOND TRANCHE												
THIRD TRANCHE												

Queries:	**Clarifications:**
1. Please consider revisiting the qualifications and experience of resources to be deployed in this project. The mindset of IT or IT Security professionals are operational and the focus is on systems availability. While Cybersecurity professional's mindset is risk based.	1. We note the suggestion but we will retain the qualifications of the resources to be involved in the project as the scope will focus on the current state of DBM's cybersecurity postures. The resources are identified based on the need to look at the operational aspects of the DBM's IT hardware/infrastructure, software, IT governance, and policies, to determine the maturity of the DBM, in terms of cybersecurity.
2. Consider revisiting the scope of the TOR and align the technical specifications with the objectives stated in the bid.	2. We note the suggestion but we will retain the scope of work as the same covers all the pertinent areas for assessment and activities to be undertaken to determine the DBM cybersecurity postures.
3. DBM to revisit and reconsider the duration of the project.	3. We note the suggestion but we will retain the duration of the project as the said timeline is aligned with the envisioned deliverables and outputs.

4. Please verify if the CIS framework requirement in the scope of work pertains to the “Center of Internet Security” which uses the 18 Critical Security Controls framework?	4. We will adopt the suggestion and correct the meaning of CIS from "Computer Information System" to "Center for Internet Security”. Please refer to the revised Terms of Reference.

5. To further assess the efforts and skillsets required for the source code review. Requesting DBM to provide what programming languages and development platforms were used on the applications?	5. The following are the programming languages that DBM uses:
	a. Typescript;
	b. Java;
	c. Javascript;
	d. Phyton;
	e. PHP;
	f. .NET; and
	g. Powerbuilder.
	
	The development platforms include Appian, Outsystems and Application Programming Interface Connect.
	
	Please refer to the revised Terms of Reference.

6. Recommended amendments for General Conditions of the Contract Clause Nos. 25.3 (a), 28, 51.1 (b), 51.1 (c), and Special Conditions of the Contract Clause No. 20.	6. The recommended amendments are denied since the wordings are based on the Philippine Bidding Documents that cannot be amended.
7. Are you expecting the winning bidder to develop a full document for following? - Business Continuity Plan - a proactive approach taken by organizations to ensure the continuation of critical business operations and services in the event of disruptions or emergencies such as natural disasters, cyber-attacks, power outages, or any unforeseen circumstances. BCP involves developing strategies, policies, and procedures to minimize the impact of such disruptions and facilitate the quick recovery and resumption of business activities. - Risk Management Plan - A Risk Management Plan is a documented approach that outlines how an organization identifies, assesses, mitigates, and monitors risks associated with its operations, projects, or initiatives. It serves as a framework for systematically managing risks and minimizing the potential negative impacts they can have on the organization's objectives and goals.	7. Yes, the DBM would require the full report for the recommended Business Continuity Plan (BCP) and Risk Management Plan based on the results of the cybersecurity postures assessment conducted. Based on the results of the cybersecurity assessment, the BCP would include recommendations on the following: a. Business Continuity Strategy (inclusive of business function recovery priorities, relocation strategy, if needed, recovery plan phases, vital records backup, restoration of physical documents when warranted, on-line access and interdependencies on systems) b. Recovery Teams (inclusive of recovery team descriptions, team assignments, personnel notification, team contacts and responsibilities) c. Recovery Procedures (inclusive of recovery activities and tasks from critical cybersecurity incident occurrence to plan activation to

A comprehensive Risk Management Plan typically includes the following key components: - Risk Identification: This involves the systematic identification and listing of potential risks that could impact the organization. It may include risks related to financial, operational, strategic, legal, regulatory, or other areas. - Risk Assessment: Once identified, risks are assessed in terms of their likelihood of occurrence and potential impact. This helps prioritize risks and determine the level of attention and resources to allocate for their mitigation. - Risk Mitigation: Risk mitigation strategies and action plans are developed to address identified risks. These strategies may include risk avoidance, risk reduction, risk transfer, or acceptance of certain risks based on a cost-benefit analysis. - Risk Monitoring and Control: Regular monitoring and reassessment of risks are integral to a Risk Management Plan. This ensures that risks are effectively managed and that new risks are identified in a timely manner. Adjustments to mitigation measures may be made based on emerging risks or changes in the organization's context. - Reporting and Communication: Effective communication of risks and the progress of risk management efforts is vital. The Risk Management Plan should outline the reporting mechanisms, stakeholders, and frequencies of reporting to keep all relevant parties informed. - Documentation and Review: The Risk Management Plan should be documented and regularly reviewed and updated as needed. This ensures that the organization maintains an ongoing awareness of risks and adapts its strategies accordingly."	alternate site operations to transition to primary operations) The scope of the risk management plan would be the results of the postures assessment which will provide information on the gaps, vulnerabilities, and technical risks related to the cybersecurity stance of the DBM. These risks will undergo the risk management process covering the following phases (among others): a. Risk Identification (inclusive of establishing context and risk criteria for cybersecurity risks) b. Risk Analysis c. Risk Evaluation d. Risk Treatment Please refer to the revised Terms of Reference.
8. Can the Firm propose more than one (1) key personnel for each required position?	8. No. Based on Section II. Instructions to Bidders of the Bidding Documents for the Project: "(d) No alternative professional staff shall be proposed, and only one Curriculum Vitae (CV) may be submitted for each position."

9. Are the shortlisted bidders required to submit TPF Nos. 6 and 12 even though the same personnel shall be nominated?	9. Yes, as required in the Checklist of Requirements for the Technical and Financial Proposal.
10. How do we accomplish the Financial Proposal Forms (FPF)?	10. The FPF forms are connected with the activities mentioned in the Technical Proposal Form (TPF) No. 8. Thus, FPF Nos. 3, 4, 5, and 6 shall have the **same number of activities** as mentioned in TPF No. 8. FPF Nos. 3, 4, 5, and 6 shall be net of taxes. FPF No. 3 is a summary of FPF Nos. 4, 5, and 6 per activity. FPF No. 2 is a summary of all activities mentioned in FPF No. 3 and shall add applicable taxes. The amount mentioned in FPF No. 1 should be equivalent to FPF No. 2.
	Note: **Attached are the following documents which should be used as part of the Bidding Documents to be submitted by the bidders:** 1. Section VI. Terms of Reference (Revised); and 2. TPF No. 8 Activity (Work) Schedule (Revised) **Attached also for Guidance of the Bidders is the Checklist of the Requirements for the Technical and Financial Proposal (Revised).**

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 December 5, 2023 right after the opening of bids.

- For guidance and information of all concerned.

Digitally signed
by Goddes
Hope O. Libiran

GODDES HOPE O. LIBIRAN
Undersecretary
Chairperson, DBM-BAC

Section VI. Terms of Reference (Revised)

1.0 PROJECT TITLE

Managed Services for Cybersecurity Posture Assessment for the Department of Budget and Management (DBM).

2.0 OBJECTIVE

The assessment typically involves a review of the organization's security policies, procedures, and technologies, as well as an evaluation of its security personnel and training programs.

The objective of this project is to identify vulnerabilities and weaknesses in an organization's security posture so that appropriate measures can be taken to address them.

3.0 TECHNICAL REQUIREMENTS

3.1. The Consultant should have their own license, implementation services, and maintenance services for the system. This will not be provided by the DBM within twelve (12) months contract period.

3.2. All applications should undergo assessment, which includes evaluating vulnerabilities in web applications, mobile applications, and desktop applications:

3.2.1. Should include a thorough examination of the network infrastructure, including firewalls, routers, switches, and other devices.

3.2.2. Should include an examination of data storage practices to ensure that sensitive data is properly secured.

3.2.3. Shall identify any weaknesses or vulnerabilities in an organization's security controls, including network devices, servers, applications, and data storage systems.

3.2.4. Shall evaluate the effectiveness of an organization's security controls, such as firewalls, intrusion detection systems, antivirus software, and access controls, to ensure they are functioning as intended.

3.2.5. Shall pinpoint potential risks to an organization's information systems and data, assess their potential impact, and develop mitigation strategies to reduce or eliminate the risks.

3.2.6. Once the assessment is complete, vulnerabilities and risks should be identified, prioritized, and addressed.

3.3. The Consultant must be able to provide a cybersecurity roadmap and reports with the following information:

3.3.1. Cybersecurity roadmap: addressing the vulnerabilities and risks identified during the assessment. The roadmap should include timelines, resources needed, and responsible parties.

3.3.2. Cyber security comprehensive report: detailing the findings of the assessment, including vulnerabilities, risks, and recommendations for improving an organization's cybersecurity posture.

4.0 SCOPE OF WORK

The following are the scope of work for this project:

4.1. The Consultant must be able to provide the assessment One (1)-time IT Security Posture Assessment of the DBM using the eighteen (18) Center for Internet Security (CIS) Critical Security Controls framework below, to establish the IT security posture baseline of the DBM:

- 4.1.1. Inventory and Control of Enterprise Assets;
- 4.1.2. Inventory and Control of Software Assets;
- 4.1.3. Data Protection;
- 4.1.4. Secure Configuration of Enterprise Assets and Software;
- 4.1.5. Account Management;
- 4.1.6. Access Control Management;
- 4.1.7. Continuous Vulnerability Management;
- 4.1.8. Audit Log Management;
- 4.1.9. Email Web Browser and Protections;
- 4.1.10. Malware Defenses;
- 4.1.11. Data Recovery;
- 4.1.12. Network Infrastructure Management;
- 4.1.13. Network Monitoring and Defense;
- 4.1.14. Security Awareness and Skills Training;
- 4.1.15. Service Provider Management;
- 4.1.16. Application Software Security;
- 4.1.17. Incident Response Management;
- 4.1.18. Penetration Testing;
- 4.1.19. Source Code Review of the following:
  - 4.1.19.1. Typescript;
  - 4.1.19.2. Java;
  - 4.1.19.3. Javascript;
  - 4.1.19.4. Phyton;
  - 4.1.19.5. PHP;
  - 4.1.19.6. .NET; and
  - 4.1.19.7. Powerbuilder

  The development platforms include Appian, Outsystems and Application Programming Interface Connect.

4.2. The Consultant shall gather information from the DBM through a series of interviews and documentation that aim to generate context and insight to the assessment. This includes, but is not limited to the DBM's network topology, systems architecture and configurations, organizational chart, security policies, and inventory of existing security controls.

4.3. The Consultant shall analyze and synthesize the results into a Gap Assessment and Recommendations Report, which shall identify strategic and tactical initiatives that build toward a defensible infrastructure and can serve as basis for the DBM’s long-term IT security program. This shall include a recommended secure architecture.

4.4. The Consultant shall provide guidance on prioritization from a technical risk perspective, subject for the approval of the DBM for execution.

4.5. The Consultant shall not be responsible for the direct implementation of recommended configuration changes on assets owned by the DBM. Further, service providers shall not have access to systems or equipment owned by the DBM.

4.6. The Consultant shall conduct an IT security gap analysis to assess the current security posture of the organization, covering the areas of people, process, and technology.

4.7. The Consultant shall utilize an industry-recognized assessment CIS framework that identifies specific and actionable steps to address the most pervasive security threats.

4.8. The Consultant shall determine if the organization's current security controls, architecture, policies, and resources are sufficient to support the target maturity level given its size, industry, and the type of information being processed and stored.

4.9. The Consultant shall provide prioritized and contextualized recommendations for the short and long terms to address the identified gaps.

4.10. The Consultant provide a recommended secure architecture for the organization.

4.11. The Consultant will provide a high-level IT security roadmap with milestones and their associated strategic and tactical initiatives.

4.12. The Consultant shall conduct the posture assessment to the internal and external-facing network services and resources of the DBM. Likewise, the scope of the posture assessment will be limited to the DBM's (production, testing, staging) environment underpinning the DBM.

4.13. The Consultant shall conduct a cybersecurity posture assessment to the Public Financial Management (PFM) Integrated Financial Management Information System (IFMIS) that will interoperate the following in a gray box approach with limited information to be shared to the penetration testers:

- 4.13.1. Convergent Gov Hub;
- 4.13.2. LGU Single Portal;
- 4.13.3. Portal Integration;
- 4.13.4. Budget Treasury Management System (BTMS);
- 4.13.5. DBM Data Center/DBM Applications;
  - 4.13.5.1. Budget Preparation Applications
    - 4.13.5.1.1. Online Submission of Budget Proposal;
    - 4.13.5.1.2. Budget Preparation Management System and Enhanced Budget Proposal Management Systems;
    - 4.13.5.1.3. National Expenditure Program;
    - 4.13.5.1.4. Government Manpower Information System;

4.13.5.1.5. Personal Services Itemization and Plantilla of Personnel, and Staffing Summary;

4.13.5.1.6. Action Document Releasing System;

4.13.5.2. Budget Legislation Applications:

4.13.5.2.1 Electronic eApproriations System

4.13.5.3. Budget Execution Applications:

4.13.5.3.1 Electronic Budget System

4.13.5.3.2 Index of Payment Computerized System

4.13.5.3.3 Electronic New Gg System

4.13.5.4. Budget Accountability Applications:

4.13.5.2.1 Unified Reporting System

4.13.5.5 Other Systems:

4.13.5.5.1 National Registry of Scripless Securities

4.13.5.5.2 Debt Management and Financial Analysis System

4.13.5.5.3 National Asset Registry System

4.13.5.5.3 Integrated Result and Risk-Based Audit Approach

4.13.5.5.4 Government Executive Information System

4.13.5.5.5 The National Government Collection and Disbursement System

4.13.5.5.6 Integrated Human Resource Information System

4.13.5.5.7 Modernized Philippine Government Electronic Procurement System Database

4.13.5.5.8 Human Resource Management Database; and

4.13.5.5.9 Authorized Government Servicing Bank Database

4.13.6. Project tools that are used by the DBM in implementing projects such as Microsoft Tools particularly MS Project, Trello and other project tools that may be utilized in the future.

4.13.7. To include the possible ten (10) application systems to be developed.

4.14. The Consultant shall have an agile methodology that involves iterative assessment sprints, where cross-functional teams continuously evaluate and improve security measures based on user stories and prioritize findings to enhance the client's cybersecurity posture. Agile principles guide transparent collaboration, enabling adaptability and responsiveness to evolving threats and priorities.

4.15. The Consultant shall have scrum framework principles that includes forming a cross-functional Scrum team to perform regular assessments, identifying vulnerabilities, and providing actionable recommendations within short, time-boxed sprints. Scrum principles foster collaboration, transparency, and incremental progress, enabling the client to continuously enhance their cybersecurity posture based on evolving threats and feedback.

5.0 QUALIFICATIONS OF THE FIRM

The managed services for the Cybersecurity Posture Assessment for the DBM shall be undertaken by a reputable Information Technology (IT) business/industry or consulting business Firm. The firm, shall have the following qualifications:

5.1. Must be in the IT business/industry or consulting business for at least (5) years based on the Bureau Internal Revenue (BIR) Certificate of Registration (COR BIR Form 2303) and/or TPF No. 10;

5.2. Must have at least 80 practicing technical IT professionals based on certified Human Resource documents;

5.3. The Consultant shall mobilize/ deploy the following five (5) personnel for the project within the Philippines based on the qualifications itemized in Annex A.1

No.	Key Personnel	Resource Count
1	Information Security Analyst	1
2	Incident Response Specialist	1
3	Managed Detection and Response Specialist	1
4	IT Security Architecture Design and Implementation Specialist	1
5	IT Security Policy Development Specialist	1

6.0 OBLIGATIONS OF THE PROCURING ENTITY

6.1. The DBM shall provide the necessary resources for the personnel to be deployed which shall include workstations, internet connection, utilities, office access, repository access, admin access, tools needed, backend software and database access as may be necessary to perform the deliverables for the project.

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

6.3. The DBM shall orient the personnel on the DBM's policies, procedures, and work assignment.

7.0 DURATION OF THE PROJECT

The project has a duration of twelve (12) months from the Notice to Proceed (NTP).

8.0 TERMS OF PAYMENT

The schedule of payment shall be based on the following milestones:

Project Activity/ Detailed Activities	Deliverables	Amount to be paid (% of Total Project Cost)	Date of Submission of Deliverables
First Tranche Project Plan Documents and Kick-Off	Inception Report ● Project Management Plan ● Project Gantt Chart and Timelines of Project Structure	20% of Total Project Cost	Month (M) 1 to M 2 Work will commence within (Thirty) 30 days upon receipt of the NTP Payment will be based on submission of Inception Reports and approval thereof by the DBM OCIO.
Second Tranche Posture Assessment Reports	Project Development (Assessments Report) ● Action Plan and Remediation Plan where it is applicable ● Agile Methodology Assessment Sprints ● Detailed Assessment Report which includes the following reports: - Risk Assessment Report - Technical Recommendations Report - Training Recommendations Report - Gap Assessment	40% of Total Project Cost	M 3 to M 8 From the approval of the Tranche 1 Deliverables Payment will be based on submission of Users Acceptance Test Report for the Project Development Phase and approval thereof by the DBM OCIO
Third Tranche System Go-Live and Stabilization	Full Implementation Plan for Project Completion ● Risk Management Plan with results of the postures assessment which will provide information on the gaps, vulnerabilities, and technical risks related to the cybersecurity stance of the DBM. These risks will undergo the risk management process covering the following phases (among others): - Risk Identification (inclusive of establishing context and risk criteria for cybersecurity risks) - Risk Analysis - Risk Evaluation - Risk Treatment ● Business Continuity Plan which includes recommendations on the following: - Business Continuity Strategy (inclusive of business function recovery priorities, relocation strategy, if needed, recovery plan phases, vital records backup, restoration of physical documents when warranted, on-line access and interdependencies on systems); - Recovery Teams (inclusive of recovery team descriptions, team assignments, personnel notification, team contacts and responsibilities) - Recovery Procedures (inclusive of recovery activities and tasks from critical cybersecurity incident occurrence to plan	40% of Total Project Cost	M 9 to M 12 From the approval of the Tranche 2 Deliverables Payment will be based on submission of Certificate of Acceptance for the Project Completion with the following supporting documents: a. Statement of Account (SOA)/Billing Statement b. NDA and approval thereof by the DBM OCIO

	activation to alternate site operations to transition to primary operations) ● Knowledge Transfer and Presentation ● Project technical support in Go-Live implementation ● Delivery and completion of all project deliverables		

9.0 SERVICE LEVEL AGREEMENT

The Solution Provider shall conform to the requirements stated in this Service Level Agreement (SLA), which shall include the following;

Component	Description	Liquidated Damages
Provision of Reports	Must provide monthly Technical and Service Reports to be submitted every first week of the subsequent month.	1/10th of 1% of the total contract price shall be imposed for every day of delay.
Compliance with Deliverables	Must provide deliverables that are mentioned on the Section 8: Terms of Payment	1/10th of 1% of the total remaining price shall be imposed for every day of delay.

a. Liquidated damages shall be charged against any money due or which may become due to the Consultant, or collected from any securities or warranties posted by the Consultant. Once the maximum is reached, the procuring entity reserves the right to rescind the contract, without prejudice to other courses of action and remedies open to it.

TPF 8. Activity (Work) Schedule

(Revised)

	Month											
	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th
Activity (Work)												
First Tranche												
Second Tranche												
Third Tranche												

CHECKLIST OF REQUIREMENTS FOR THE TECHNICAL AND FINANCIAL PROPOSAL

(Revised)

Class "A" Documents

Technical Proposal consisting of the following as described in ITB item 10 (C. Preparation of Bids):

□ **TPF 1. Technical Proposal Submission Form**

□ **TPF 2. Consultant's References**

□ **TPF 3. Comments and Suggestions of Consultant on the Terms of Reference and on Data, Services and Facilities to be provided by the Procuring Entity**

□ **TPF 4. Description of the Methodology and Work Plan for Performing the Project**

□ **TPF 5. Team Composition and Task Projects**

□ **TPF 6. Curriculum Vitae for Proposed Professional Staff**

· Training Certificate, Diploma, Employment Certificate, and other related Certifications may be submitted

□ **TPF 7. Time Schedule for Professional Staff**

□ **TPF 8. Activity (Work) Schedule**

□ **TPF 9. Omnibus Sworn Statement**

· Accompanied by the company's Secretary's Certificate or Special Power of Attorney

□ **TPF 12. Statement of the Consultant's Nationality**

□ **Bid Security** as described in ITB clause 15 (see Bid Securing Declaration Form)

Financial Proposal as described in ITB clause 11 (C. Preparation of Bids):

□ **FPF 1. Financial Proposal Submission Form**

□ **FPF 2. Summary of Costs**

□ **FPF 3. Breakdown of Price per Activity**

□ **FPF 4. Breakdown of Remuneration per Activity**

□ **FPF 5. Reimbursables per Activity**

□ **FPF 6. Miscellaneous Expenses**

***Should there be any discrepancy between the requirements stated in the Checklist and the requirements specified in the Bidding Documents, the latter shall prevail.**