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 October 20, 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 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>PARTICULARS</th><th>AMENDMENTS</th></tr>
<tr><td>Section III. Eligibility Data Sheet

<table>
<tr><th>Eligibility Documents</th><td></td></tr>
<tr><td>9.2</td><td>xxx

<table>
<tr><th>No.</th><th>Evaluation Criteria</th></tr>
<tr><td></td><td>xxx</td></tr>
<tr><td>1.1.2</td><td>With substantial number of practicing technical IT professionals based on certified Human Resource documents</td></tr>
<tr><td></td><td>With more than 150 practicing technical IT professionals based on certified Human Resource documents</td></tr>
<tr><td></td><td>With more than 100-150 practicing technical IT professionals based on certified Human Resource documents</td></tr>
<tr><td></td><td>With less than 100 practicing technical IT professionals based on certified Human Resource documents</td></tr>
</table></td></tr>
</table></td><td>Section III. Eligibility Data Sheet

<table>
<tr><th>Eligibility Documents</th><td></td></tr>
<tr><td>9.2</td><td>xxx

<table>
<tr><th>No.</th><th>Evaluation Criteria</th></tr>
<tr><td></td><td>xxx</td></tr>
<tr><td>1.1.2</td><td>With substantial number of practicing technical IT professionals based on certified Human Resource documents</td></tr>
<tr><td></td><td>With more than ~~150~~ 90 practicing technical IT professionals based on certified Human Resource documents</td></tr>
<tr><td></td><td>With more than ~~100-150~~ 81-90 practicing technical IT professionals based on certified Human Resource documents</td></tr>
<tr><td></td><td>With ~~less than 100~~ 80 practicing technical IT professionals based on certified Human Resource documents</td></tr>
</table></td></tr>
</table></td></tr>
</table>

		xxx			xxx
	2.1.2.	Experience in the Cybersecurity Industry:		2.1.2.	Experience in the Cybersecurity Industry:
	2.1.2.1	Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation		2.1.2.1	Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation
		• Five (5) years or more Cybersecurity Industry experience			• ~~Five (5)~~ **NINE (9)** years or more Cybersecurity Industry experience
		• Less than five (5) years of experience in any Cybersecurity Industry			• **WITH 6-8 YEARS OF EXPERIENCE IN ANY CYBERSECURITY INDUSTRY**
					• ~~Less than~~ **F**ive (5) years of experience in any Cybersecurity Industry
	2.1.3	Certifications		2.1.3	Certifications**:** **CERTIFIED INFORMATION SECURITY MANAGER (CISM), CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) AND INTERNATIONAL INFORMATION**
		• Both Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA)			
		• Either CISM or CISA			

					SYSTEM SECURITY CERTIFICATION CONSORTIUM, INC. (ISC2)
					• **HAVE ALL THREE KINDS OF CERTIFICATIONS**
					• ~~Both Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA)~~ **HAVE TWO KINDS OF CERTIFICATIONS**
					• ~~Either CISM or CISA~~ **HAVE ONLY ONE OF THE CERTIFICATIONS**
		2.2	Incident Response Specialist	2.2	Incident Response Specialist
			Educational Qualification	**2.2.1**	Educational Qualification
			xxx		xxx
		2.2.1	Experience in the Cybersecurity Industry:	~~2.2.1~~ **2.2.2**	Experience in the Cybersecurity Industry:
			Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and		Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and

		Incident Response and Preparation			Incident Response and Preparation
		• Five (5) years or more Cybersecurity Industry experience			• ~~Five (5)~~ **NINE (9)** years or more Cybersecurity Industry experience
		• Less than five (5) years of experience in any Cybersecurity Industry			• **WITH 6-8 YEARS OF EXPERIENCE IN ANY CYBERSECURITY INDUSTRY**
					• ~~Less than~~ **F**ive (5) years of experience in any Cybersecurity Industry
	2.2.2	Certifications		~~2.2.2~~ **2.2.3**	Certifications**: CISM, CISA AND ISC2**
		• Both CISM or CISA			• **HAVE ALL THREE KINDS OF CERTIFICATIONS**
		• Either CISM or CISA			• ~~Both Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA)~~ **HAVE TWO KINDS OF CERTIFICATIONS**
					• ~~Either CISM or CISA~~ **HAVE ONLY ONE OF THE CERTIFICATIONS**
		xxx			xxx

	2.3.2	Experience in the Cybersecurity Industry:		2.3.2	Experience in the Cybersecurity Industry:
		Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation			Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation
		• Five (5) years or more Cybersecurity Industry experience			• ~~Five (5)~~ **NINE (9)** years or more Cybersecurity Industry experience
		• Less than five (5) years of experience in any Cybersecurity Industry			• **WITH 6-8 YEARS OF EXPERIENCE IN ANY CYBERSECURITY INDUSTRY**
					• ~~Less than~~ **F**ive (5) years of experience in any Cybersecurity Industry
	2.3.3	Certifications		2.3.3	Certifications**: CISM, CISA AND ISC2**
		• Both CISM or CISA			• **HAVE ALL THREE KINDS OF CERTIFICATIONS**
		• Either CISM or CISA			• ~~Both Certified Information Security Manager (CISM) and Certified Information~~

					~~Systems Auditor (CISA)~~ **HAVE TWO KINDS OF CERTIFICATIONS**
					• ~~Either CISM or CISA~~ **HAVE ONLY ONE OF THE CERTIFICATIONS**
	2.4	IT Security Architecture Design and Implementation Specialist		2.4	IT Security Architecture Design and Implementation Specialist
		Educational Qualification		**2.4.1**	Educational Qualification
		xxx			xxx
	2.4.1	Experience in the Cybersecurity Industry:		~~2.4.1~~ **2.4.2**	Experience in the Cybersecurity Industry:
		Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation			Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation
		• Five (5) years or more Cybersecurity Industry experience			• ~~Five (5)~~ **NINE (9)** years or more Cybersecurity Industry experience
		• Less than five (5) years of experience in any Cybersecurity Industry			• **WITH 6-8 YEARS OF EXPERIENCE IN ANY CYBERSECURITY INDUSTRY**

					• ~~Less than~~ **F**ive (5) years of experience in any Cybersecurity Industry
	2.4.2	Certifications		~~2.4.2~~ **2.4.3**	Certifications**: CISM, CISA AND ISC2**
		• Both CISM or CISA			• **HAVE ALL THREE KINDS OF CERTIFICATIONS**
		• Either CISM or CISA			• ~~Both Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA)~~ **HAVE TWO KINDS OF CERTIFICATIONS**
					• ~~Either CISM or CISA~~ **HAVE ONLY ONE OF THE CERTIFICATIONS**
	2.5	IT Security Policy Development Specialist		2.5	IT Security Policy Development Specialist
		Educational Qualification		**2.5.1**	Educational Qualification
		xxx			xxx
	2.5.1	Experience in the Cybersecurity Industry:		~~2.5.1~~ **2.5.2**	Experience in the Cybersecurity Industry:
		Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and			Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability

			Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation				Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation
			• Five (5) years or more Cybersecurity Industry experience				• ~~Five (5)~~ **NINE (9)** years or more Cybersecurity Industry experience
			• Less than five (5) years of experience in any Cybersecurity Industry				• **WITH 6-8 YEARS OF EXPERIENCE IN ANY CYBERSECURITY INDUSTRY**
							• ~~Less than~~ **F**ive (5) years of experience in any Cybersecurity Industry
		2.3.5	Certifications			2.3.5	Certifications**: CISM, CISA AND ISC2**
			• Both CISM or CISA				• **HAVE ALL THREE KINDS OF CERTIFICATIONS**
			• Either CISM or CISA				• ~~Both Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA)~~ **HAVE TWO KINDS OF CERTIFICATIONS**
							• ~~Either CISM or CISA~~ **HAVE ONLY ONE OF THE**

			CERTIFICATIONS

Section III. Bid Data Sheet

ITB Clause	
10.2	In addition to the TPFs mentioned, the shortlisted Consultants shall submit the following: TPF 10 – Statement of all Government and Private Contracts Completed; and TPF 11 – List of all Ongoing Government and Private Contracts Including Contracts Awarded but no yet Started TPF 12 – Statement of Consultant's Nationality
25.3	xxx **Evaluation Criteria** xxx B. Work Experience (related to the project) 1) Information Security Analyst Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation • Five (5) years or more Cybersecurity Industry experience • Less than five (5) years of experience in any Cybersecurity Industry

Section III. Bid Data Sheet

ITB Clause	
~~10.2~~	~~In addition to the TPFs mentioned, the shortlisted Consultants shall submit the following:~~ ~~TPF 10 – Statement of all Government and Private Contracts Completed; and~~ ~~TPF 11 – List of all Ongoing Government and Private Contracts Including Contracts Awarded but no yet Started~~ ~~TPF 12 – Statement of Consultant's Nationality~~
25.3	xxx **Evaluation Criteria** xxx B. Work Experience (related to the project) 1) Information Security Analyst Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation • ~~Five (5)~~ **NINE (9)** years or more Cybersecurity Industry experience • **WITH 6-8 YEARS OF EXPERIENCE IN ANY CYBERSECURITY INDUSTRY**

2) Incident Response Specialist	2) Incident Response Specialist
Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation	Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation
• Five (5) years or more Cybersecurity Industry experience	• ~~Five (5)~~ **NINE (9)** years or more Cybersecurity Industry experience
• Less than five (5) years of experience in any Cybersecurity Industry	• **WITH 6-8 YEARS OF EXPERIENCE IN ANY CYBERSECURITY INDUSTRY**
	• ~~Less than~~ **F**ive (5) years of experience in any Cybersecurity Industry
3) Managed Detection and Response Specialist	3) Managed Detection and Response Specialist
Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation	Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation
• Five (5) years or more Cybersecurity Industry experience	• ~~Five (5)~~ **NINE (9)** years or more Cybersecurity Industry experience
• Less than five (5) years of experience in any Cybersecurity Industry	• **WITH 6-8 YEARS OF EXPERIENCE IN ANY CYBERSECURITY INDUSTRY**

4) IT Security Architecture Design and Implementation on Specialist	4) IT Security Architecture Design and Implementation on Specialist
Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation	Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation
• Five (5) years or more Cybersecurity Industry experience	• ~~Five (5)~~ **NINE (9)** years or more Cybersecurity Industry experience
• Less than five (5) years of experience in any Cybersecurity Industry	• **WITH 6-8 YEARS OF EXPERIENCE IN ANY CYBERSECURITY INDUSTRY**
	• ~~Less than~~ **F**ive (5) years of experience in any Cybersecurity Industry
5) IT Security Policy Development Specialist	5) IT Security Policy Development Specialist
Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation	Experience in any Cybersecurity Industry of the following Industry Managed Detection and Response, Advanced Vulnerability Assessment and Penetration Testing, Compromise Assessment, Secure Code Audit and Incident Response and Preparation
• Five (5) years or more Cybersecurity Industry experience	• ~~Five (5)~~ **NINE (9)** years or more Cybersecurity Industry experience
• Less than five (5) years of experience in any Cybersecurity Industry	• **WITH 6-8 YEARS OF EXPERIENCE IN ANY CYBERSECURITY INDUSTRY**
	• ~~Less than~~ **F**ive (5) years of experience in any Cybersecurity Industry

	• ~~Less than~~ **F**ive (5) years of experience in any Cybersecurity Industry
B. Certification	B. Certifications**: CERTIFIED INFORMATION SECURITY MANAGER (CISM), CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) AND INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM, INC. (ISC2)**
1) Information Security Analyst	1) Information Security Analyst
Both Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA) and Certified Information Systems Auditor (CISA)	**HAVE ALL THREE KINDS OF CERTIFICATIONS**
	~~Both Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA)~~ **HAVE TWO KINDS OF CERTIFICATIONS**
Either CISM or CISA	~~Either CISM or CISA~~ **HAVE ONLY ONE OF THE CERTIFICATIONS**
2) Incident Response Specialist	2) Incident Response Specialist
Both CISM and CISA	**HAVE ALL THREE KINDS OF CERTIFICATIONS**
	~~Both CISM and CISA~~ **HAVE TWO KINDS OF CERTIFICATIONS**
Either CISM or CISA	~~Either CISM or CISA~~ **HAVE ONLY ONE OF THE CERTIFICATIONS**
3) Managed Detection and Response Specialist	3) Managed Detection and Response Specialist
Both CISM and CISA	**HAVE ALL THREE KINDS OF CERTIFICATIONS**
	~~Both CISM and CISA~~ **HAVE TWO KINDS OF CERTIFICATIONS**
Either CISM or CISA	~~Either CISM or CISA~~ **HAVE ONLY ONE OF THE CERTIFICATIONS**

4) IT Security Architecture Design and Implementation on Specialist	4) IT Security Architecture Design and Implementation on Specialist
Both CISM and CISA	**HAVE ALL THREE KINDS OF CERTIFICATIONS**
Either CISM or CISA	~~Both CISM and CISA~~ **HAVE TWO KINDS OF CERTIFICATIONS**
	~~Either CISM or CISA~~ **HAVE ONLY ONE OF THE CERTIFICATIONS**
5) IT Security Policy Development Specialist	5) IT Security Policy Development Specialist
Both CISM and CISA	**HAVE ALL THREE KINDS OF CERTIFICATIONS**
Either CISM or CISA	~~Both CISM and CISA~~ **HAVE TWO KINDS OF CERTIFICATIONS**
xxx	~~Either CISM or CISA~~ **HAVE ONLY ONE OF THE CERTIFICATIONS**
	xxx
A. Years in the Information Technology Business	A. Years in the Information Technology Business
With 10 years or more in the IT business	With ~~10~~ **NINE (9)** years or more in the IT business
With 6 - 9 years in the IT Business	With 6 - ~~9~~ **8** years in the IT Business
With 5 years in the IT Business	With 5 years in the IT Business
B. With substantial number of practicing technical IT professionals based on certified Human Resource documents	B. With substantial number of practicing technical IT professionals based on certified Human Resource documents
With more than 150 practicing technical IT professionals based on certified Human Resource documents	With more than ~~150~~ **90** practicing technical IT professionals based on certified Human Resource documents
With 100-150 practicing technical IT professionals based on certified Human Resource documents	With more than ~~100-150~~ **81-90** practicing technical IT professionals based on certified Human Resource documents
With less than 100 practicing technical IT professionals based on certified Human Resource documents	With ~~less than 100~~ **80** practicing technical IT professionals based on certified Human Resource documents

Section IV. Terms of Reference	Section IV. Terms of Reference (Revised)
xxx	xxx
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 following are the objectives of this project: • To identify vulnerabilities and weaknesses in an organization's security posture so that appropriate measures can be taken to address them and; • To identify potential weaknesses and vulnerabilities before they can be exploited by cyber attackers.	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 following are the objectives of this project:~~ • ~~To identify vulnerabilities and weaknesses in an organization's security posture so that appropriate measures can be taken to address them and;~~ • ~~To identify potential weaknesses and vulnerabilities before they can be exploited by cyber attackers.~~ **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	3.0 TECHNICAL REQUIREMENTS
xxx	xxx
3.1. The Consultant shall be obliged to provide license, implementation services, and maintenance of the system within twelve (12) months contract period.	3.1. The Consultant ~~shall be obliged to provide~~ **SHOULD HAVE THEIR OWN** license, implementation services, and maintenance **SERVICES** ~~of~~ **FOR** the system. **THIS WILL NOT BE PROVIDED BY THE DBM** within **THE** twelve (12) month contract period.
4.0 SCOPE OF WORK	4.0 SCOPE OF WORK
xxx	xxx
4.1.18. Penetration Testing. xxx	4.1.18. Penetration Testing~~.~~; 4.1.19. **SOURCE CODE REVIEW.**

	xxx
4.13.5.5.9 Authorized Government. Servicing Bank Database	4.13.5.5.9 Authorized Government~~.~~ Servicing Bank Database
xxx	xxx
4.13.7. To be included the possible ten (10) application systems to be developed.	4.13.7. To ~~be included~~ **INCLUDE** the possible ten (10) application systems to be developed.
xxx	xxx
5.0 QUALIFICATIONS OF THE FIRM	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) Firm. The firm, shall have the following qualifications:	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 Information Technology business for at least (5) years based on the Bureau Internal Revenue (BIR) Certificate of Registration (COR BIR Form 2303).	5.1. Must be in the ~~Information Technology~~ **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 100 practicing technical IT professionals based on certified Human Resource documents;	5.2. Must have at least ~~100~~ **80** practicing technical IT professionals based on certified Human Resource documents;
xxx	xxx
8.0 TERMS OF PAYMENT	8.0 TERMS OF PAYMENT

Project Activity/ Detailed Activities	Deliverables	Amount to be paid (% of Total Project Cost)	Date of Submission of Deliverables
First Tranche xxx	Inception Report • Project Management Plan • Risk Management	xxx	xxx

Project Activity/ Detailed Activities	Deliverables	Amount to be paid (% of Total Project Cost)	Date of Submission of Deliverables
First Tranche xxx	Inception Report • Project Management Plan • ~~Risk Management~~	xxx	xxx

	and Business Continuity Plan • Project Gantt Chart and Timelines of Project Structure		
Second Tranche xxx	Project Development (Assessments Report) • Action Plan • Remediation Plan • Agile Methodology Assessment Sprints • Detailed Assessment Report • Risk Assessment Report • Posture Assessment Report • Executive Summary Reports • Analysis and Report Documentation • Technical Recommendations Report • Training Recommendations Report • Gap Assessment and Recommendations Report Submission	xxx	xxx

	~~and Business Continuity Plan~~ • Project Gantt Chart and Timelines of Project Structure		
Second Tranche xxx	Project Development (Assessments Report) • Action Plan **AND REMEDIATION PLAN WHERE IT IS APPLICABLE** • ~~Remediation Plan~~ • Agile Methodology Assessment Sprints • Detailed Assessment Report **WHICH INCLUDES THE FOLLOWING REPORTS:** • ~~Risk Assessment Report~~ • ~~Posture Assessment Report~~ • ~~Executive Summary Reports~~ • ~~Analysis and Report Documentation~~ • ~~Technical Recommendations Report~~ • ~~Training Recommendations Report~~ • ~~Gap Assessment and Recommendations Report Submission~~ - **RISK ASSESSMENT REPORT**	xxx	xxx

Third Tranche xxx	Full Implementation Plan for Project Completion xxx	xxx	xxx

9.0 SERVICE LEVEL AGREEMENT

xxx

a. Liquidated damages shall be charged against any money due or which may become due to the contractor, or collected from any securities or warranties posted by the contractor. 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.

	- **TECHNICAL RECOMMENDATIONS REPORT** - **TRAINING RECOMMENDATIONS REPORT** - **GAP ASSESSMENT**		
Third Tranche xxx	Full Implementation Plan for Project Completion • **RISK MANAGEMENT AND BUSINESS CONTINUITY PLAN** xxx	xxx	xxx

9.0 SERVICE LEVEL AGREEMENT

xxx

a. Liquidated damages shall be charged against any money due or which may become due to the ~~contractor~~ **CONSULTANT**, or collected from any securities or warranties posted by the ~~contractor~~ **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.

Annex A.1
Qualifications and Responsibilities of the Personnel to be Deployed for the Project

Particulars	Qualifications
Information Security Analyst	xxx • Must be either Certified Information Security Manager (CISM) or Certified Information Systems Auditor (CISA) or both.
Incident Response Specialist	xxx • Must be either CISM or CISA or both
Managed Detection and Response Specialist	xxx • Must be either CISM or CISA or both
IT Security Architecture Design and Implementation Specialist	xxx • Must be either CISM or CISA or both
IT Security Policy Development Specialist	xxx • Must be either CISM or CISA or both

TPF 6. Format of Curriculum Vitae (CV) for Proposed Professional Staff

xxx

Photocopy of the following documents must be submitted together with the Curriculum Vitae to evidence educational attainment, work experience and professional certifications:

xxx

Annex A.1
Qualifications and Responsibilities of the Personnel to be Deployed for the Project
(Revised)

Particulars	Qualifications
Information Security Analyst	xxx • Must be either Certified Information Security Manager (CISM)**,** ~~or~~ Certified Information Systems Auditor (CISA)**,** ~~or both~~ **AND/OR HAS CERTIFICATION FROM INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM, INC. (ISC2)**.
Incident Response Specialist	xxx • Must be either CISM**,** ~~or~~ CISA**,** ~~or both~~ **AND/OR HAS CERTIFICATION FROM ISC2**.
Managed Detection and Response Specialist	xxx • Must be either CISM**,** ~~or~~ CISA**,** ~~or both~~ **AND/OR HAS CERTIFICATION FROM ISC2**.
IT Security Architecture Design and Implementation Specialist	xxx • Must be either CISM**,** ~~or~~ CISA**,** ~~or both~~ **AND/OR HAS CERTIFICATION FROM ISC2**.
IT Security Policy Development Specialist	xxx • Must be either CISM**,** ~~or~~ CISA**,** ~~or both~~ **AND/OR HAS CERTIFICATION FROM ISC2**.

TPF 6. Format of Curriculum Vitae (CV) for Proposed Professional Staff
(Revised)

xxx

Photocopy of the following documents ~~must~~ **MAY** be submitted together with the Curriculum Vitae to evidence educational attainment, work experience and professional certifications:

xxx

TPF 9. Omnibus Sworn Statement [Jurat] [Format shall be based on the latest Rules on Notarial Practice]	**TPF 9. Omnibus Sworn Statement (Revised)** ~~[Jurat]~~ ~~[Format shall be based on the latest Rules on Notarial Practice]~~ **SUBSCRIBED AND SWORN TO BEFORE ME IN [PLACE OF EXECUTION], PHILIPPINES ON THIS [DATE OF NOTARIZATION], AFFIANT EXHIBITING BEFORE ME HIS COMPETENT EVIDENCE OF IDENTITY [VALID IDENTIFICATION ISSUED BY THE GOVERNMENT].** **NOTARY PUBLIC** **DOC. NO. _____;** **PAGE NO. _____;** **BOOK NO. _____;** **SERIES OF _____.**
Bid Securing Declaration Form [Jurat] [Format shall be based on the latest Rules on Notarial Practice]	**Bid Securing Declaration Form (Revised)** ~~[Jurat]~~ ~~[Format shall be based on the latest Rules on Notarial Practice]~~ **SUBSCRIBED AND SWORN TO BEFORE ME IN [PLACE OF EXECUTION], PHILIPPINES ON THIS [DATE OF NOTARIZATION], AFFIANT EXHIBITING BEFORE ME HIS COMPETENT EVIDENCE OF IDENTITY [VALID IDENTIFICATION ISSUED BY THE GOVERNMENT].** **NOTARY PUBLIC** **DOC. NO. _____;** **PAGE NO. _____;** **BOOK NO. _____;** **SERIES OF _____.**
TPF 10. Statement of all Government and Private Contracts Completed which are Similar in Nature xxx Instructions: a) Projects should be completed within five (5) years immediately preceding December 5, 2023.	**TPF 10. Statement of all Government and Private Contracts Completed which are Similar in Nature (Revised)** xxx Instructions: a) Projects should be completed within five (5) **TO TEN (10)** years immediately preceding ~~December 5~~ **OCTOBER 27**, 2023.

TPF 11. List of all Ongoing Government and Private Contracts Including Contracts Awarded but not yet Started xxx Instructions: i. State all ongoing contracts including those awarded but not yet started (government and private contracts which may be similar or not similar to the project being bidded) prior to December 5, 2023.	**TPF 11. List of all Ongoing Government and Private Contracts Including Contracts Awarded but not yet Started** **(Revised)** xxx Instructions: i. State all ongoing contracts including those awarded but not yet started (government and private contracts which may be similar or not similar to the project being bidded) prior to ~~December 5~~ **OCTOBER 27**, 2023.
Queries:	**Clarifications:**
1. Clarifications on the 10 application systems to be developed.	1. Please refer to the revised Item 4.13.7 of the Terms of Reference.
2. Scope of work – re-align the scope of work (cyber posture assessment) to objectives and duration. 12 months is too long for an assessment only; Engineering, SECOps and development of security policies and related documents are too big as a value added. Such, recalibrating the scope of work is highly recommended.	2. Scope of work is retained and duration of the project is retained due to rolling out of the Budget Treasury and Management System (BTMS) in the 3rd Quarter of 2024.
3. Project objectives – suggest to revisit since objectives 1 & 2 are the same.	3. Second bullet in the Objective is deleted. Please refer to the revised Terms of Reference.
4. Vendor and professionals qualification – open the opportunity to Consulting Firm. Consider the number of completed contracts of vendors on top of number of years in the Industry. As for the professional – consider the number of similar projects involvement, cyber related certifications and roles in the completed similar projects.	4. Revised qualifications of the Firm to include IT business or IT consulting industry business. Please refer to the revised Terms of Reference.
5. For organizational level assessment – consider other frameworks outside CIS, such as ISO27001/02, NIST, Data Privacy Act, OWASP, etc.	5. CIS framework is retained since the focus is more on the cybersecurity postures of DBM.
6. For systems level assessment – further elaborate the test procedures e.g., VAPT testing, OS hardening benchmarking, etc.	6. Test procedures would include all tools needed to come up with the postures agreement.
7. Reports – need to revisit and re-group some expected deliverables for more clarity.	7. Please refer to the revised reports required under Item 8.0 of the Terms of Reference.

8. Please revisit the requirement "Risk Management and Business Continuity Plan" it includes various stages such as planning, analysis, implementation, testing, and refinement. 2 months will not be enough for this requirement. 9. Please elaborate the requirement of license, implementation, and maintenance services. How is this relevant the objective of this bid?	8. Please refer to the revised reports required under Item 8.0 of the Terms of Reference. 9. The consultant should be using with their own licenses and tools, and no longer provided by the DBM.
	Note: **<u>Attached are the following documents which should be used as part of the Bidding Documents to be submitted by the bidders:</u>** **1. Section VI. Terms of Reference (Revised);** **2. TPF 6. Format of Curriculum Vitae (CV) for Proposed Professional Staff (Revised);** **3. TPF 9. Omnibus Sworn Statement (Revised);** **4. Bid Securing Declaration Form (Revised);** **5. TPF 10. Statement of all Government and Private Contracts Completed which are Similar in Nature (Revised); and** **6. TPF 11. List of all Ongoing Government and Private Contracts Including Contracts Awarded but not yet Started (Revised)** **<u>Attached also for Guidance of the Bidders are the following:</u>** **7. Checklist of Eligibility Documents (for shortlisting purposes); and** **8. Checklist of the requirements for the Technical and Financial Proposal**

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 October 27, 2023 right after the opening of bids.

- For guidance and information of all concerned.

RAMON VICENTE B. ASUNCION
Director IV
Vice 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) Computer Information System (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.

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 and Business Continuity Plan ● Knowledge Transfer and Presentation ● Project technical support in Go-Live implementation ● Delivery and completion of all project deliverables	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

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.

Annex A.1
Qualification and Responsibilities of the Personnel to be Deployed for the Project
(Revised)

No.	Particulars	Resource Count	Qualifications	Tasks
			The following should have the list of qualifications:	
1	Information Security Analyst	One (1)	• At least a Bachelor's Degree in Information Technology related courses such as Computer Science, Information Technology, Computer Engineering, Information Science, and Data Science • Must have at least five (5) years of experience in the Cybersecurity industry with related background capabilities in any of the following; ○ Managed Detection and Response ○ Advanced Vulnerability Assessment and Penetration Testing ○ Compromise Assessment, ○ Secure Code Audit ○ Incident Response and Preparation • Must be either Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), and/or has certification from International Information System Security Certification Consortium, Inc. (ISC2).	Information Security Analysts are responsible for: ● Identifying and assessing security risks ● Developing and implementing information security policies and procedures, ensuring compliance with data privacy regulations ● Conducting security awareness training, responding to and managing security incidents, monitoring and auditing security controls ● Performing vulnerability assessments, and contributing to the overall security governance of the organization, all while maintaining a strong focus on safeguarding data, protecting against cyber threats, and minimizing risks associated with information security, data privacy, and risk management.

2	Incident Response Specialist	One (1)	● At least a Bachelor's Degree in Information Technology related courses such as Computer Science, Information Technology, Computer Engineering, Information Science, and Data Science. ● Must have at least five (5) years of experience in the Cybersecurity Industry with related background and capabilities in any of the following: ○ Managed Detection and Response ○ Advanced Vulnerability Assessment and Penetration Testing ○ Compromise Assessment, ○ Secure Code Audit ○ Incident Response and Preparation • Must be either CISM, CISA, and/or has certification from ISC2.	Incident Response Specialists are tasked with: ● Promptly and effectively responding to security incidents by leading incident response teams ● Coordinating the containment and mitigation of threats ● Conducting digital forensics investigations ● Analyzing the impact and scope of incidents, documenting findings, communicating incident details to stakeholders, ● Implementing incident response plans ● Recommending security improvements, and continually enhancing incident response procedures to minimize the impact of security breaches and maintain the organization's cyber resilience.
3	Managed Detection and Response Specialist	One (1)	● At least a Bachelor's Degree in Information Technology related courses such as Computer Science, Information Technology, Computer Engineering, Information Science, and Data Science. ● Must have at least (5) years of experience in in the Cybersecurity Industry with related background and capabilities in any of the following: ○ Managed Detection and Response	Managed Detection and Response (MDR) Specialists are responsible for: ● Proactively monitoring an organization's IT environment, including networks, endpoints, and applications, to detect and respond to security threats and incidents. ● Tasks involve configuring and managing security monitoring tools, analyzing security alerts and anomalies, ● Conducting threat hunting to identify advanced threats ● Coordinating incident response efforts,

			○ Advanced Vulnerability Assessment and Penetration Testing ○ Compromise Assessment, ○ Secure Code Audit ○ Incident Response and Preparation • Must be either CISM, CISA, and/or has certification from ISC2.	fine-tuning detection rules and strategies ● Providing real-time threat intelligence, collaborating with clients to tailor MDR services to their specific needs, and continuously improving the organization's security posture by staying informed about emerging threats and evolving MDR technologies and practices.
4	IT Security Architecture Design and Implementation Specialist	One (1)	● At least a Bachelor's Degree in Information Technology related courses such as Computer Science, Information Technology, Computer Engineering, Information Science, and Data Science. ● Must have at least five (5) years of experience in the Cybersecurity Industry with a related background and capabilities in any of the following: ○ Managed Detection and Response ○ Advanced Vulnerability Assessment and Penetration Testing ○ Compromise Assessment, ○ Secure Code Audit ○ Incident Response and Preparation ○ Application Security, Network Security, • Must be either CISM, CISA, and/or has certification from ISC2.	IT Security Architecture Design and Implementation Specialists are responsible for: ● Designing and deploying comprehensive security architectures that align with an organization's strategic goals and protect against cyber threats. ● Evaluating existing security measures, identifying vulnerabilities, defining security requirements, developing security solutions and strategies, selecting and implementing security technologies (such as firewalls, IDS/IPS, encryption, and access controls), ● Ensuring integration with existing IT infrastructure ● Conducting security assessments and audits ● Collaborating with cross-functional teams to secure applications and data, and staying current with emerging security threats and industry best practices to continually enhance the organization's security posture.

5	IT Security Policy Development Specialist	One (1)	● At least a Bachelor's Degree in Information Technology related courses such as Computer Science, Information Technology, Computer Engineering, Information Science, and Data Science. ● Must have at least five (5) years of experience in Cybersecurity Industry with related background and capabilities any of the following; ○ Managed Detection and Response ○ Advanced Vulnerability Assessment and Penetration Testing ○ Compromise Assessment, ○ Secure Code Audit ○ Incident Response and Preparation • Must be either CISM, CISA, and/or has certification from ISC2.	IT Security Policy Development Specialists are responsible for: ● Creating and maintaining robust information security policies and procedures within organizations ● Assessing regulatory requirements and industry standards to ensure compliance ● Collaborating with stakeholders to define security policies, guidelines, and standards ● Developing comprehensive security documentation, conducting security awareness and training programs ● Facilitating policy implementation and enforcement, monitoring policy adherence ● Responding to security incidents by applying relevant policies, and continuously reviewing and updating policies to align with evolving cybersecurity threats and technologies while fostering a culture of security within the organization.

TPF 6. FORMAT OF CURRICULUM VITAE (CV) FOR PROPOSED PROFESSIONAL STAFF (REVISED)

Proposed Position: _____

Name of Firm: _____

Name of Staff: _____

Profession: _____

Date of Birth: _____

Years with Firm/Entity: _____ Nationality: _____

Membership in Professional Societies: _____

_____

Detailed Tasks Assigned: _____

_____

Key Qualifications:

[*Give an outline of staff member's experience and training most pertinent to tasks on project. Describe degree of responsibility held by staff member on relevant previous projects and give dates and locations. Use about half a page.*]

Experience in the Information Technology Industry (Start from the most recent)							
Company	**Project**	**Date**		**Position**	**Location**	**Area of Expertise** (e.g Cybersecurity/ Business Intelligence/Web Based Development/ API Development)	**Actual Duties and Responsibilities**
		From	To				
1.							
2.							
3.							
4.							
5.							
6.							
7.							

Signature of Authorized Signatory: _____

Relevant Trainings (Start from the most recent)- please attach training certificate					
Course Title	**Date**		**Location**	**No of Hours.**	**Conducted/ Sponsored by**
	From	To			
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Relevant Certifications (Start from the most recent)- please attach copy of certificates			
Certification	**Valid Date**		**Certification Issued by**
	From	To	
1.			
2.			
3.			
4.			

Education:

[*Summarize college/university and other specialized education of staff members, giving names of schools, dates attended, and degrees obtained. Use about one quarter of a page.*]

Education (Start from the most recent)			
School	**Inclusive Date**		**Degree Course**
	From	To	
1.			
2.			
3.			

Employment Record:

[*Starting with present position, list in reverse order every employment held. List all positions held by staff member since graduation, giving dates, names of employing organizations, titles of positions held, and locations of projects. For experience in last ten years, also give types of activities performed and client references, where appropriate. Use about two pages.*]

Work Experience (Start from the most recent)					
Company	**Inclusive Date**		**Total** (Years, Months)	**Position Title**	**Actual Duties and Responsibilities**
	From	To			
1.					
2.					
3.					

Note:

Photocopy of the following documents may be submitted together with the Curriculum Vitae to evidence educational attainment, work experience and professional certifications:

Signature of Authorized Signatory: _____

1. Certificate of Employment and similar documents (e.g., certificate of engagement)
2. Training programs attended
3. Diploma
4. Professional Certifications and/or Licenses

Certification:

I, the undersigned, certify that to the best of my knowledge and belief, these data correctly describe me, my qualifications, and my experience.

Commitment:

I also commit to work for the Project in accordance with the time schedule as indicated in the contract once the firm is awarded the Project.

_____Date: _____
[Signature of staff member and authorized representative of the firm] *Day/Month/Year*

Full name of staff member: _____
Full name of authorized representative: _____

SUBSCRIBED AND SWORN to before me this __ day of *[month] [year]* at *[place of execution]*, Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her *[insert type of government identification card used]*, with his/her photograph and signature appearing thereon, with no. _____.

Witness my hand and seal this ___ day of *[month] [year]*.

NAME OF NOTARY PUBLIC

Serial No. of Commission _____
Notary Public for _____ until _____
Roll of Attorneys No. _____
PTR No. __, *[date issued], [place issued]*
IBP No. __, *[date issued], [place issued]*
Doc. No. ___
Page No. ___
Book No. ___
Series of ____.

TPF 9. OMNIBUS SWORN STATEMENT (REVISED)

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _____) S.S.

A F F I D A V I T

I, *[Name of Affiant]*, of legal age, *[Civil Status]*, *[Nationality]*, and residing at *[Address of Affiant]*, after having been duly sworn in accordance with law, do hereby depose and state that:

1. ***Select one, delete the other:***

   If a sole proprietorship: I am the sole proprietor or authorized representative of *[Name of Consultant]* with office address at *[address of Consultant]*;

   If a partnership, corporation, cooperative, or joint venture: I am the duly authorized and designated representative of *[Name of Consultant]* with office address at *[address of Consultant]*;

2. ***Select one, delete the other:***

   If a sole proprietorship: As the owner and sole proprietor or authorized representative of *[Name of Consultant]*, I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for *[Name of the Project]* of the *[Name of the Procuring Entity]* *[insert* "as shown in the attached duly notarized Special Power of Attorney" *for authorized representative]*;

   If a partnership, corporation, cooperative, or joint venture: I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for *[Name of the Project]* of the *[Name of the Procuring Entity]*, accompanied by the duly notarized Special Power of Attorney, Board/Partnership Resolution, or Secretary's Certificate, whichever is applicable*;*

3. *[Name of Consultant]* is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board;

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. *[Name of Consultant]* is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. ***Select one, delete the rest:***

   If a sole proprietorship: The owner or sole proprietor is not related to the Head of the Procuring Entity, procurement agent if engaged, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   If a partnership or cooperative: None of the officers and members of *[Name of Bidder]* is related to the Head of the Procuring Entity, procurement agent if engaged, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   If a corporation or joint venture: None of the officers, directors, and controlling stockholders of *[Name of Consultant]* is related to the Head of the Procuring Entity, procurement agent if engaged, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Consultant]* complies with existing labor laws and standards; and

8. *[Name of Consultant]* is aware of and has undertaken the following responsibilities as a Bidder:

   a) Carefully examine all of the Bidding Documents;

   b) Acknowledge all conditions, local or otherwise, affecting the implementation of the Contract;

   c) Made an estimate of the facilities available and needed for the contract to be bid, if any; and

   d) Inquire or secure Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.

9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

10. In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.

IN WITNESS WHEREOF, I have hereunto set my hand this_____day of_____, 20 ___at _____ Philippines.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

SUBSCRIBED AND SWORN to before me in *[place of execution]*, Philippines on this *[date of notarization]*, affiant exhibiting before me his competent evidence of identity *[valid identification issued by the government]*.

NOTARY PUBLIC

Doc. No. _____;
Page No. _____;
Book No. _____;
Series of _____.

Bid-Securing Declaration

(Revised)

[shall be submitted with the Bid if bidder opts to provide this form of bid security]

(REPUBLIC OF THE PHILIPPINES)
CITY OF _____) S.S.
x----------x

BID SECURING DECLARATION
Project Identification No.: *DBM-2024-06*

To: *[Insert name and address of the Procuring Entity]*
I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid-Securing Declaration.

2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting Order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of written demand by the procuring entity for the commission of acts resulting to the enforcement of the bid securing declaration under Sections 23.1(b), 34.2, 40.1 and 69.1, except 69.1 (f), of the IRR of RA 9184; without prejudice to other legal action the government may undertake.

3. I/We understand that this Bid-Securing Declaration shall cease to be valid on the following circumstances:

    a. Upon expiration of the bid validity period, or any extension thereof pursuant to your request;
    b. I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right;
    c. I am/we are declared as the bidder with the Highest Rated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this__day of *[month] [year]* at *[place of execution]*.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

SUBSCRIBED AND SWORN to before me in *[place of execution]*, Philippines on this *[date of notarization]*, affiant exhibiting before me his competent evidence of identity *[valid identification issued by the government]*.

NOTARY PUBLIC

Doc. No. _____;
Page No. _____;
Book No. _____;
Series of _____.

TPF 10. Statement of all Government and Private Contracts Completed which are Similar in Nature (Revised)

Business Name: _____
Business Address:_____

Name of Client/Contact Person/Contact Number/Email Address	Date of the Contract	Kinds of Consulting Services	Amount of Contract	Date of Delivery	End User's Acceptance or Official Receipt(s) Issued for the Contract
Government					
Private					

Submitted by : _____
(Printed Name and Signature)

Designation : _____

Date : _____

Instructions:

a) Projects should be completed within five (5) to ten (10) years immediately preceding October 27, 2023.

b) Completed contract:
   (i) Similar contracts shall refer to the delivery, provision, and deployment of services that provide evaluation and assessment of security status or risks of an organization's networks, information, and systems.
   (ii) If there is no similar completed contract in a year, state **none** or equivalent term. This shall not be a basis for disqualification.

c) Please note that item 6.4 of the Government Procurement Policy Board (GPPB) Circular No. 04-2020 dated September 16, 2020 states that, "[t]he PEs shall check **compliance of the submitted forms with the mandatory provisions stated above**. **Non-submission of the Required Forms or non-inclusion of the mandatory provisions in any of the Required Forms shall be a ground for disqualification**."

Moreover, GPPB Non-Policy Matter Opinion No. 041-2014 dated October 9, 2014 partially states that "**even contracts that include non-disclosure agreements or confidentiality clauses are required to be disclosed**. It is likewise good to clarify that the requirement refers to a "statement" to be made by the bidder relative to all its ongoing and private contracts, and not the actual submission of the physical contracts."

TPF 11. List of all Ongoing Government and Private Contracts Including Contracts Awarded but not yet Started (Revised)

Business Name: _____
Business Address:_____

Name of Client/ Contact Person/ Contact Number/ Email Address	Date of the Contract	Kinds of Consulting Services	Value of Outstanding Contracts	Date of Delivery
Government				
Private				

Submitted by : _____
(Printed Name and Signature)
Designation : _____

Date : _____

Instructions:

i. State all ongoing contracts including those awarded but not yet started (government and private contracts which may be similar or not similar to the project being bidded) prior to October 27, 2023.
ii. If there is no ongoing contract including awarded but not yet started as of the aforementioned period, state none or equivalent term.
Please note that item 6.4 of the Government Procurement Policy Board (GPPB) Circular No. 04-2020 dated September 16, 2020 states that, "[t]he PEs shall check **compliance of the submitted forms with the mandatory provisions stated above**. **Non-submission of the Required Forms or non-inclusion of the mandatory provisions in any of the Required Forms shall be a ground for disqualification**."

Moreover, GPPB Non-Policy Matter Opinion No. 041-2014 dated October 9, 2014 partially states that "**even contracts that include non-disclosure agreements or confidentiality clauses are required to be disclosed**. It is likewise good to clarify that the requirement refers to a "statement" to be made by the bidder relative to all its ongoing and private contracts, and not the actual submission of the physical contracts."

CHECKLIST OF ELIGIBILITY REQUIREMENTS

ELIGIBILITY AND SHORTLISTING

Class "A" Documents

Legal Documents

☐ (a) Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages);

Technical Documents

☐ (b) Eligibility Documents Submission Form accompanied by a duly notarized company's Secretary's Certificate or Special Power of Attorney, as applicable (See form) ; **and**

☐ (c) Curriculum Vitae for the Proposed Professional Staff (Use TPF 6); **and**

☐ (d) Statement of all Government and Private Contracts Completed which are Similar in Nature (TPF 10); **and**

☐ (e) Certificate of Good Standing and Satisfactory Completion or equivalent document (for Completed Contracts); **and**

☐ (f) List of all Ongoing Government and Private Contracts Including Contracts Awarded but not yet Started (Use TPF 11); **and**

☐ (g) Statement of the Consultant's Nationality (Use TPF 12); **and**

☐ (h) Photocopy of the following documents may be submitted together with the Curriculum Vitae to evidence educational attainment, work experience and professional certifications:

1. Certificate of Employment and similar documents (e.g. certificate of engagement)
2. Training programs attended
3. Diploma
4. Professional Certifications and/or Licenses

Class "B" Documents

Legal Documents

☐ (i) Valid Joint Venture Agreement (JVA) if JV is in existence or duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the event that the bid is successful.

*** In case a discrepancy exists between the requirements stated in the Checklist and the requirements specified in the Bidding Documents, the latter shall prevail.**

CHECKLIST OF REQUIREMENTS FOR THE TECHNICAL AND FINANCIAL PROPOSAL

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
- ☐ **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.**