




Republic of the Philippines
COURT OF TAX APPEALS
Quezon City

APPROVED FOR POSTING

FROM : _____

TO : _____

Approved By: _____


REQUEST FOR QUOTATION

**CONDUCT OF IN-HOUSE TRAINING ON COMPREHENSIVE PRIVACY, INFORMATION
SYSTEMS AUDITING, CONTROL AND SECURITY**

Date : June 22, 2023

RFQ No. : 23-2023

Name of Company : _____
Address : _____
Business Permit No. : _____
TIN No. : _____
PhilGEPS Registration No. : _____

The Court of Tax Appeals (CTA) intends to engage a training provider of known qualifications for the **Conduct of In-house Training on Comprehensive Privacy, Information Systems Auditing, Control and Security**, through Section 53.9 (Negotiated Procurement – Small Value Procurement) of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184, as amended.

Please quote your best offer for the conduct of the training course described on the **Technical Specifications** below, subject to the Terms and Conditions provided at the dorsal portion of this Request for Quotation (RFQ).

Submit your quotation duly signed by you or your authorized representative and copies of the following eligibility requirements not later than **June 27, 2023**:

1. Mayor's/ Business Permit;
2. PhilGEPS Registration Number or PhilGEPS Registration Certificate;
3. Notarized Omnibus Sworn Statement (with Secretary's Certificate, if a corporation or Certificate of Partnership Resolution, if a partnership);
4. Income/ Business Tax Return; and
5. Manifestation of compliance to the attached Technical Specifications.

Open quotations may be submitted at the address indicated below or sent through email at ppmd.cta@judiciary.gov.ph or ppmd.cta@gmail.com.


ANNE BENITA S. AUSTIN
Chief Judicial Staff Officer

Procurement and Property Management Division

After having carefully read and accepted the Technical Specifications and the General Terms and Conditions, I/We submit our quotation/s:

Project Description	Quantity	Approved Budget for the Contract (ABC)	OFFER <i>(Amount to be filled-up by the Supplier)</i>
Conduct of In-house Training on Comprehensive Privacy, Information Systems Auditing, Control and Security <i>(Please indicate your compliance with the Technical Specifications attached in this Request for Quotation (RFQ).)</i>	One (1) Lot	Seven Hundred Sixteen Thousand Eight Hundred Pesos (₱716,800.00)	<hr/> <i>(It is understood that the above-quoted offer is inclusive of all applicable government taxes.)</i>

(Signature over Printed Name)

(Company Name)

(Telefax, Landline and/or Cellphone Number)

(E-mail Address)

TECHNICAL SPECIFICATIONS

Conduct of In-house Training on Comprehensive Privacy, Information Systems Auditing, Control and Security

The Training Provider must write **Comply** in the column **Statement of Compliance** opposite each of the individual parameter of each Requirement:

Item	CTA Requirements	Statement of Compliance
1	<p>The Conduct of In-house Training on Comprehensive Privacy, Information Systems Auditing, Control and Security must be conducted every Friday, from 8:00am to 5:00pm starting on July 14, 2023, and have a total duration of at least seventy-two (72) hours.</p> <p>The 10-day Course shall provide the participants:</p> <ul style="list-style-type: none"> • In-depth learning of the concepts and principles of privacy, information systems auditing, control and security reinforced by practical approaches in the control and assurance of IT-enabled operating environment; and • Practical approach in conducting IT audit that can be readily used by the participants after all the sessions. <p>The Course shall be conducted in-house in a classroom setting.</p>	
2	<p>The Training Provider:</p> <ul style="list-style-type: none"> • Must be PhilGEPS Accredited; • Must have at least five (5) years of experience; • Shall submit the Curriculum Vitae (CV) and relevant Certifications [Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in Risk and Information Systems Control® (CRISC®), Certified Data Privacy Solutions Engineer™ (CDPSE®), etc.] of each resource speaker; • Shall provide training materials and certificates of participation/completion to participants; • Shall submit to CTA (end user) copies of presentations after each session; and • Shall facilitate Certification sample questions, mock exam, and workshop. 	
3	<p>Session 1: Information Systems Auditing Process</p> <p>Date : July 14, 2023 Duration : 8 hours Number of Pax : 16 - 20</p> <p>Session Objectives: <i>The resource speaker should be able to train the participants on how to:</i></p> <ul style="list-style-type: none"> • <i>Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization.</i> • <i>Conduct an audit in accordance with Information System (IS) audit standards and a risk based IS audit strategy.</i> • <i>Communicate audit progress, findings, results and recommendations to stakeholders.</i> • <i>Conduct audit follow-up to evaluate whether risk has been sufficiently addressed.</i> • <i>Evaluate IT management and monitoring of controls.</i> • <i>Utilize data analytics tools to streamline audit processes.</i> • <i>Provide consulting services and guidance to the organization to improve the quality and control of information systems.</i> • <i>Identify opportunities for process improvement in the organization's IT policies and practices</i> 	

Item	CTA Requirements	Statement of Compliance
	<p>Session 2: Information Systems Acquisition, Development, and Implementation</p> <p>Date : July 21, 2023 Duration : 8 hours Number of Pax : 16 – 20</p> <p>Session Objectives: <i>The resource speaker should be able to train the participants on how to:</i></p> <ul style="list-style-type: none"> • Evaluate whether the business case for proposed changes to information systems meet business objectives. • Evaluate the organization's project management policies and practices. • Evaluate controls at all stages of the information system development life cycle. • Evaluate the readiness of information systems for implementation and migration into production. • Conduct post-implementation review of systems to determine whether project deliverables, controls and requirements are met. • Evaluate change, configuration, release, and patch management policies and practices. <p>Session 3: Governance and Management of IT</p> <p>Date : July 28, 2023 Duration : 8 hours Number of Pax : 16 – 20</p> <p>Session Objectives: <i>The resource speaker should be able to train the participants on how to:</i></p> <ul style="list-style-type: none"> • Evaluate the IT strategy for alignment with the organization's strategies and objectives. • Evaluate the effectiveness of IT governance structure and IT organizational structure. • Evaluate the organization's management of IT policies and practices. • Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements. • Evaluate IT resource and portfolio management for alignment with the organization's strategies and objectives. • Evaluate the organization's risk management policies and practices. • Evaluate IT management and monitoring of controls. • Evaluate the monitoring and reporting of IT key performance indicators (KPIs). • Evaluate whether IT supplier selection and contract management processes align with business requirements. • Evaluate whether IT service management practices align with business requirements. • Conduct periodic review of information systems and enterprise architecture. • Evaluate data governance policies and practices. • Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives. • Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices. <p>Session 4. Information Systems Operations and Business Resilience</p> <p>Date : August 4, 2023 Duration : 8 hours Number of Pax : 16 – 20</p> <p>Session Objectives: <i>The resource speaker should be able to train the participants on how to:</i></p> <ul style="list-style-type: none"> • Evaluate the organization's ability to continue business operations. • Evaluate whether IT service management practices align with business requirements. • Conduct periodic review of information systems and enterprise architecture. 	

Item	CTA Requirements	Statement of Compliance
	<ul style="list-style-type: none"> • Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization objectives. • Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization's objectives. • Evaluate database management practices. • Evaluate data governance policies and practices. • Evaluate problem and incident management policies and practices • Evaluate change, configuration, release, and patch management policies and practices. • Evaluate end-user computing to determine whether the processes are effectively controlled. • Evaluate policies and practices related to asset life cycle management. <p>Session 5. Protection of Information Assets</p> <p>Date : August 11, 2023 Duration : 8 hours Number of Pax : 16 – 20</p> <p>Session Objectives: The resource speaker should be able to train the participants on how to:</p> <ul style="list-style-type: none"> • Evaluate problem and incident management policies and practices. • Evaluate the organization's information security and privacy policies and practices. • Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded. • Evaluate logical security controls to verify the confidentiality, integrity, and availability of information. • Evaluate data classification practices for alignment with the organization's policies and applicable external requirements. • Evaluate policies and practices related to asset life cycle management. • Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives. • Perform technical security testing to identify potential threats and vulnerabilities. • Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices. <p>Session 6. Information Security Governance</p> <p>Date : August 18, 2023 Duration : 8 hours Number of Pax : 16 – 20</p> <p>Session Objectives: The resource speaker should be able to train the participants on how to:</p> <ul style="list-style-type: none"> • Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program; • Establish and/or maintain an information security governance framework to guide activities that support the information security strategy; • Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program; • Establish and maintain information security policies to guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives; • Develop business cases to support investments in information security; • Identify internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) to ensure that these factors are continually addressed by the information security strategy; 	

Item	CTA Requirements	Statement of Compliance
	<ul style="list-style-type: none"> • Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy; • Define, communicate and monitor information wear, responsibilities throughout the organization (e.g. data, owners, data custodians, end users, privileged or high-risk users) and lines of authority; and • Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy. <p>Session 7. Information Risk Management</p> <p>Date : August 25, 2023 Duration : 8 hours Number of Pax : 16 – 20</p> <p>Session Objectives: The resource speaker should be able to train the participants on how to:</p> <ul style="list-style-type: none"> • Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value. • Identify legal, regulatory, organizational, and other applicable requirements to manage the risk of noncompliance to acceptable levels. • Ensure that risk assessments, vulnerability assessments and threat analyses are conducted consistently, and at appropriate times, to identify and assess risk to the organization's information. • Identify, recommend, or implement appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite. • Determine whether information security controls are appropriate and effectively manage risk to an acceptable level. • Facilitate the integration of information risk management into business and IT processes (e.g., systems development, procurement, project management) to enable a consistent and comprehensive information risk management program across the organization. • Monitor for internal and external factors (e.g., threat landscape, cybersecurity, geopolitical, regulatory change) that may require reassessment of risk to ensure that changes to existing or new risk scenarios are identified and managed appropriately. <p>Session 8. Data Privacy Fundamentals/Compliance Data Privacy</p> <p>Date : September 1, 2023 Duration : 8 hours Number of Pax : 16 – 20</p> <p>Session Objectives: The resource speaker should be able to train the participants on how to:</p> <ul style="list-style-type: none"> • Provide audit services of an organization's privacy environment with the acquired knowledge and information on the following: <ul style="list-style-type: none"> ✓ Data Privacy Principles ✓ Rights of the Data Subject ✓ Data Privacy Officer (DPO) ✓ Compliance Requirements ✓ Data Protection Framework ✓ Breach Reporting ✓ Compliance Scenarios ✓ Data Privacy Frameworks ✓ Privacy and the Business ✓ Auditing Data Privacy 	

Item	CTA Requirements	Statement of Compliance
	<ul style="list-style-type: none"> ✓ <i>Information Auditor's Role</i> ✓ <i>Audit Work Program</i> <p>Session 9. Mock Exam</p> <p>Date : September 8, 2023 Duration : 4 hours Number of Pax : 16 – 20</p> <p>Session 10. Workshop</p> <p>Date : September 15, 2023 Duration : 8 hours Number of Pax: 16 – 20</p>	

I hereby certify to comply and deliver the above requirements:

Name of Company/ Training Provider	Signature over Printer Name	Date
---------------------------------------	-----------------------------	------

GENERAL TERMS AND CONDITIONS

1. Training Provider shall provide correct and accurate information in this form.
2. The price quotation/s must be valid for a period of thirty (30) calendar days from the date of submission.
3. Price quotation/s, to be denominated in Philippine peso shall include taxes, duties and/or levies payable.
4. Quotations exceeding the Approved Budget for the Contract shall be rejected.
5. Any interlineations, erasures or overwriting shall be valid only if they are signed or initialed by you or any of your authorized representative/s.
6. Award of Contract shall be made to the lowest quotation which complies with the Technical Specifications and other terms and conditions stated therein.
7. Representatives from the Personnel Development Committee (PDC), Committee on Records Management and Information Service (CRMIS) and Procurement and Property Management Division (PPMD) of the CTA shall have the right to evaluate and inspect the training service rendered to confirm their conformity with the Technical Specifications.
8. Payment shall be made thirty (30) days from receipt of the billing statement.
9. The CTA reserves the right to accept or reject any offer, to annul the procurement process, and to reject offers at any time prior to the award of contract, without thereby incurring any liability to the affected Suppliers.