

TERMS OF REFERENCE

SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF QUEZON CITY CYBER SECURITY SYSTEM

I. RATIONALE AND BRIEF BACKGROUND

The Quezon City Local Government is one amongst all of the cities which was recognized for utilizing the best practice for digital transformation in delivering an efficient and effective modern service for their constituents and citizens of the Philippines.

Quezon City, like any other city, has sensitive information that needs to be protected from unauthorized access. This includes personal information of citizens, financial data, and other confidential data that needs to be kept secure.

Considering complex information systems and other pertinent data amongst different offices and departments of the Quezon City LGU we seek to invest in an opportunity that is deemed necessary and to have the assistance of a third party service provider which is capable of delivering a system design which is efficient, holistic and secure.

Cyber attacks are becoming increasingly common and sophisticated. A cyber attack can cause significant damage to the city's infrastructure, disrupt essential services, and lead to financial losses.

II. PROJECT DESCRIPTION

The project involves effective cybersecurity measures which can help prevent attacks and minimize the potential damage to the city's digital services.

Overall, cybersecurity is essential for Quezon City to protect its sensitive information, prevent cyber attacks, comply with regulations, and enhance its reputation.

Test the organization's ability to respond to a cyber-attack and evaluate how effective the cyber incident response plans are.

To assess and identify the vulnerabilities of the organization's cyber security defense, allowing the organization to strengthen and improve its defenses against real-world cyber attacks.

III. **PROJECT SCOPE OF WORK**

The Service provider shall deliver the following:

A. Table Top Exercises

1. Analyze the differences between documented processes, expected responses and determine the reasons for the discrepancies and provide a plan to address them.
2. The exercises are based on real-world scenarios which are relevant to the organization.
3. The program should be rapid, efficient, and non-intrusive to operations.
4. The provider has been operating in the cyber security space for more than ten years and conducting Tabletop Exercises for more than five years.
5. The Exercises should cover executive strategies in responding to a cyber crisis.
6. Ability to conduct roundtable exercises simulating relevant real-world scenarios and be flexible to pivot to different inputs to observe the organization's actions and decisions in response.
7. Facility to conduct prework to understand the organization's threat profile, operational environment, and particular areas of concern to develop more accurate scenarios.
8. Ability to execute the exercises either remotely or on site.
9. The outcome of the exercise to be presented at an executive level and audience.
10. The exercise should be managed by a project manager with additional subject matter experts executing the tasks.
11. Must have performed more than 300 Red Team Assessments each year

B. Red Teaming (RT)

1. Security Principal/Vendor must have proven track records in delivering RT across industry sectors globally in the last 10 years.
2. Security Principal/Vendor must have its own RT that perform over 400 RT assessments per year.
3. Security Principal/Vendor must have its own RT that perform over 400 RT assessments per year.
4. Security Principal/Vendor must have global operations in US, Europe, Japan, Asia Pacific regions.
5. Security Principal/Vendor must have extensive threat intel network to facilitate in the execution of the RT exercise.
6. Security Principal/Vendor must have a proven RT methodology which can be tracked during the exercise and also customized for the customer.
7. Security Principal/Vendor must be able to help develop a remediation plan following the outcome of the RT exercise to address weaknesses identified.

8. Security Principal/Vendor should be able to provide a detailed report targeted at different audiences with understandable analysis and actionable recommendations.
9. Security Principal/Vendor must be able to provide an intelligence led RT exercise in partnership with the requirements set by the customer.
10. Security Principal/Vendor must be able to provide realistic capture flags using various levels of techniques.
11. Security Principal/Vendor should have the ability to replay the RT exercise to the customer's security operations.
12. The RT exercise must be able to deliver a threat profile which is specific for the customer covering the following at the very least:
 - a. Cyber threat landscape changes over the last 3 year period.
 - b. Newly identified tactics, techniques and procedures (TTPs)
 - c. New threat actors
 - d. Incident report on 1c
13. Conduct research and analysis on the intelligence output from 12 and requirements set by the customer in order to establish genuine TTPs.
14. Identify targets for the scope of the RT exercise covering both digital and non-digital assets.
15. Conduct the project initiation with the customer key stakeholders in a controlled need to know basis which can be executed in line with the customer's preferred method.
16. Clearly articulate the techniques utilized to exploit the customer environment.
17. Reporting should be in detail and cover the following:
 - a. Testing Scenarios
 - b. Scenarios Outcome
 - c. Customer Environment Restoration
 - d. Gaps and Remediation Recommendations
18. Up to one week of retesting on the completion of the remediation activities.

IV. **PROJECT STANDARDS AND REQUIREMENTS**

The following are the minimum qualifications and requirements for the Supplier or Bidder:

- i. Track Record
 - a. The service provider must be in the same industry as per their DTI or SEC filing for at least nine (9) years.
 - b. The service provider must be an operational company for at least nine (9) years.
 - c. The service provider must have satisfactorily implemented a similar project of cloud-hosting, web application firewall and security services within the last three (3) years.

- d. The service provider should have implemented a public sector cloud-hosting web application firewall and security services project with a single completed contract amounting to at least fifty percent (50%) of the ABC.

ii. Organization

- a. The service provider must have updated Platinum status in PHILGEPS.
- b. The service provider must be a duly registered company with a DTI or SEC filing.
- c. The service provider must be filed with DTI or SEC as an IT company with the purpose of software development and the supply of IT-related goods and services.
- d. The service provider must have an active and updated registration with the National Privacy Commission.
- e. The service provider must be a PREMIER/highest level partnership certificate. The bidder will be required to submit the appropriate Partnership Level certification from its associated Cloud Service Provider.
- f. The service provider shall guarantee that the system shall abide with the DATA PRIVACY ACT OF 2012 to ensure that the personal information is protected.

iii. Manpower

The proposed project team must be composed of experts and specialists as indicated in the table below. The roster must include a minimum of six (6) distinct physical persons, with no overlapping of functions. However, the service provider has the option to add more personnel depending on his work strategy. The bid document must include curriculum vitae of proposed manpower with work experience related to Information System development.

STAFF

- a. One (1) Project Manager
 - At least four (4) years experience in managing IT related projects; solutioning of cyber security threats.
 - Graduate of any 4-year computer course or IT related course.
 - Must have a certificate on cloud digital leader.
- b. Two (2) Red Team Service providers
 - Extensive penetration testing background across applications and infrastructure;
 - Threat modeling experience when planning a Red Team engagement;
 - Red Teaming engagements should include government agencies;
 - Graduate of any 4-year computer course or IT related course (Minimum);
 - Professional certifications in the areas of penetration testing;
 - Public presentations on cyber security is an advantage;
 - Identification of vulnerability disclosures (CVE) is an advantage;

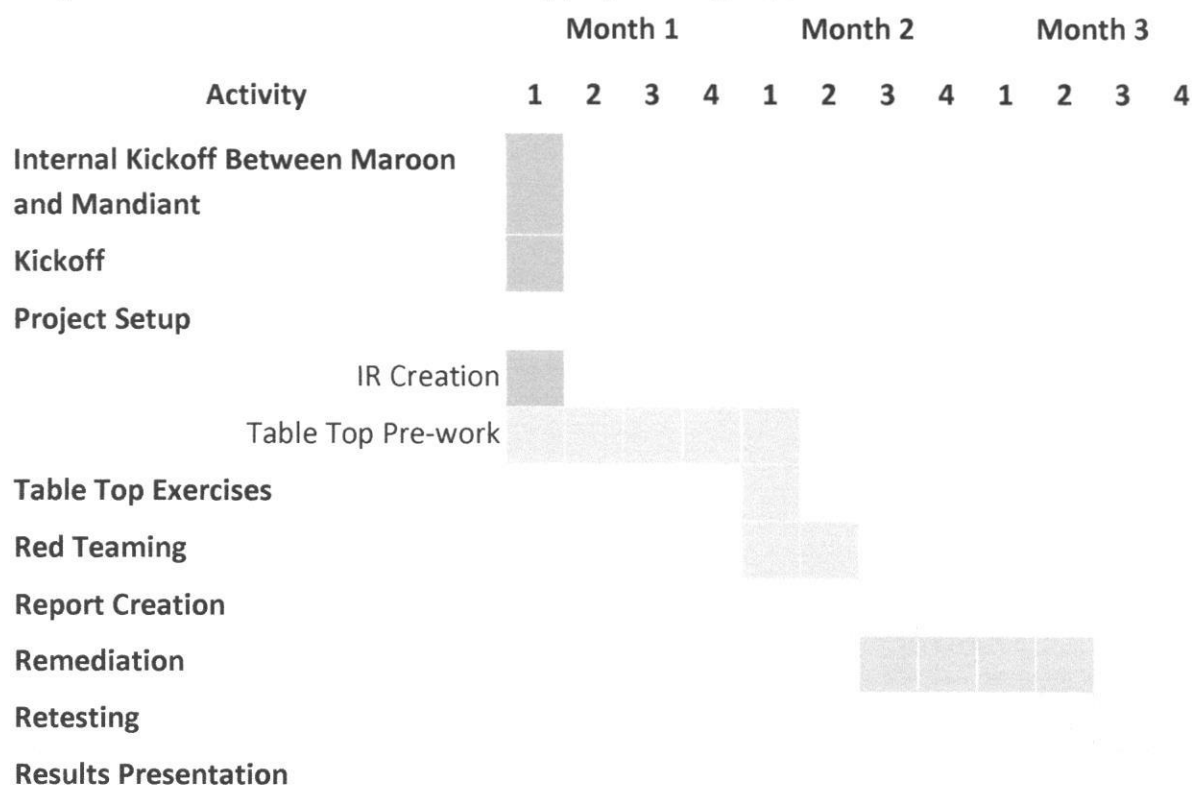
- Have at least Ten (10) years' experience in security testing and performing network penetration testing.
- c. Two (2) Table Top Exercise Service provider(s)
- Experience in design, build and operationalizing modern security operation centers (SOC);
 - Table Top Exercise engagements should include government agencies;
 - Graduate of any 4-year computer course or IT related course (Minimum);
 - Professional certifications in information and cyber security;
 - Have at least Ten (10) years' experience in security operations centers (SOCs), cyber defense and computer incident response team (CIRT)

V. PROJECT DEVELOPMENT AND DEPLOYMENT DURATION

The duration of the contract is ninety (90) calendar days upon issuance of the Notice to Proceed. The service provider shall work in close coordination with the personnel of Quezon City Cyber Security. The service provider is not required to physically report to the Office. However, regular meetings and workshops will be conducted with the QCLGU and other concerned offices for any update and support either through personal or virtual meetings, whenever feasible.

Project Implementation Plan

Project Timeline: Twelve weeks or Ninety (90) working days



VI. APPROVED BUDGET COST

The Approved Budget for the Contract (ABC) amounts to Fourteen Million Pesos Only (P14,000,000.00) (VAT inclusive).

COST DERIVATION

Type	Count	Cost
Red Teaming	1	
Table Top Exercises	1	
Sub-total		
Documentation, Training Module and Training		
Technical & Customer Service Support		
Grand Total (VAT Inc.)		₱ 14,000,000.00

VII. DELIVERY AND PAYMENT SCHEDULE

The project shall be paid on the schedule indicated below:

Project Activity/Milestone	Deliverables	Amount of Payment/ Payment Schedule
1. Table top exercise	<ul style="list-style-type: none">Kindly refer to <i>Scope of Work and Deliverables</i> listed items.	<ul style="list-style-type: none">40% of the Total Project Cost(30) days upon sign off table top.
2. Red Teaming (RT)	<ul style="list-style-type: none">Kindly refer to <i>Scope of Work and Deliverables</i> listed items.	<ul style="list-style-type: none">40% of the Total Project Cost(30) days upon sign off Red teaming.
3. Report creation	<ul style="list-style-type: none">To deliver documentation and reporting of findings.	<ul style="list-style-type: none">10% of the Total Project Cost(30) days upon sign off of Report creation.
4. Review report & Remediation	<ul style="list-style-type: none">QC LGU to conduct remediation on their system.	<ul style="list-style-type: none">n/aTimeline: Twenty-one (21) calendar days after repo.
5. Retesting	<ul style="list-style-type: none">Mandiant to conduct retesting upon completion of the remediation.	<ul style="list-style-type: none">5% of the Total Project Cost(30) days upon sign off of retesting report.
6. Result Presentation	<ul style="list-style-type: none">To present results to stakeholders.	<ul style="list-style-type: none">5% of the Total Project Cost(30) days upon sign off of the presentation report.

PRINCIPAL SOLUTION CAPABILITIES (PS)

1. The PS must have at least 15 years of experience in incident response and forensic investigations related to cyber security across various countries and verticals.
2. The PS must have a global team of service providers of 300 or more dedicated to incident response and compromised assessment.
3. The PS must have a global team of incident investigators located in at least 20 countries.
4. The PS must have its own Threat Intel Team of at least 200 or more cyber threat intelligence analysts generating market leading intel.
5. The PS must have cumulative experience of 100,000 hours per year in cyber security investigations.
6. The PS must have deep knowledge of attack methodologies, background, objectives, target countries/verticals categorized by specific APT groups.
7. The PS must be able to provide profiles of at least 10 APT groups with comprehensive insights built on tracking of and responding to threats/breaches originating from these APT groups.
8. The PS must be at the forefront of all the latest threat campaigns, often being called upon in the media to discuss the threat impact to organizations and offer credible and relevant recommendations.
9. The PS must have done 1000+ incident response engagements per year.
10. The PS must be rated a Leader in Incident Response by Forrester Wave (Q1 2022).
11. The PS must be rated a Leader in External Threat Intelligence Services by Forrester Wave (Q1 2021).
12. The PS must have at least 500 frontline experts.
13. The PS must have 18 Million+ Endpoints monitored globally.
14. The PS must have 2000 Threat Actors tracked.
15. Have performed at least Malware Detonations in the order of millions per hour.
16. A leader in Threat Intel with at least 15K threat intel reports published annually.

ADDITIONAL DOCUMENTS

1. Certified Data Privacy Officer by NPC
2. Valid National Privacy Commission Certificate or Official Receipt as proof of renewal for CY 2023
3. The bidder must have the following:
 - a. One (1) Certified Development Operations Engineer – college graduate (preferably IT-related courses) and with at least five (5) years experience on this industry
 - b. Three (3) Certified Cloud Architect – college graduate (preferably IT-related courses) and with at least two (2) years experience on this industry
 - c. One (1) Cloud Security Engineer – college graduate (preferably IT-related courses) and with at least one (1) year experience on this industry
 - d. Four (4) cloud developer – college graduate (preferably IT-related courses) and with at least two (2) years experience on this industry
4. The bidder must have a highest level of Partnership with its principal

VIII. **BASIS OF PAYMENT**

Upon confirmation by QC LGU City Administrator Office of the availability & deployment of the cyber security service, the QC LGU City Administrator Office will release One hundred percent (100%) per milestone accomplished and indicated on the *DELIVERY AND PAYMENT SCHEDULE* amount to the service provider.

IX. **PENALTIES FOR BREACH OF CONTRACT**

Failure to deliver the services according to the standards and requirements set by the City shall constitute an offense and shall subject the Contractor to penalties and/or liquidated damages pursuant to RA 9184 and its revised Implementing Rules and Regulations.



X. **CANCELLATION OR TERMINATION OF CONTRACT**

The guidelines contained in RA 9184 and its revised IRR shall be followed in the termination of any service contract. In the event the City terminated the Contract due to default insolvency, or for cause, it may enter negotiated procurement pursuant to RA 9184 and its IRR.

Prepared by:


PAUL RENE S. PADILLA
Head, QC-ITTD

Reviewed and Endorsed by:


MICHAEL VICTOR N. ALIMURUNG
City Administrator 

Noted by:


ROWENA T. MACATAO
City Government Department Head III
Chief of Staff