REQUEST FOR PROPOSALS

RFP No: BVIPA/RFP2024/02

CONSULTANCY SERVICES FOR THE INFORMATION SYSTEMS AUDIT FOR BRITISH VIRGIN ISLANDS PORTS AUTHORITY

15 APRIL 2024

SPONSORING OFFICE

BVI Ports Authority
Pasea Place
Road Town, Tortola VG 1110
British Virgin Islands

Request for Proposals: Consultancy Services for Information Systems and Security Audit for The British Virgin Islands Ports Authority

1. INTRODUCTION

1.1. The British Virgin Islands Ports Authority (the "Ports Authority" or BVIPA) is inviting professional, experienced, competent, and resourceful firms to submit technical and financial proposals in response to this Request for Proposals (RFP) for **Consultancy Services for Information Systems and Security Audit for the British Virgin Islands Ports Authority** (hereinafter referred to the "Services").

1.2. The RFP shall be available from Tuesday**, 16 April 2024**. Interested tenderers may obtain a copy of the RFP by contacting the Board Secretary at email address jjthomas@bviports.org or may download a copy from the Ports Authority's **website at https://bvi.ports.org.**

1.3. Bidders are advised that the destination mailbox is NOT automated to send bidders a date and time acknowledgement of receipt and delivery of their message. Therefore, bidders should not assume that their email has been safely received, and it is the responsibility of the bidder to follow up with the Ports Authority using the contact information provided Section 1.5 if an acknowledgement of receipt is not received within two (2) working days of submission of their email. Under no circumstance will the Ports Authority be responsible for non-receipt of documents by bidders.

1.4. The assignment is expected to commence in **May 2024** and will be executed on a full-time basis.

1.5. The address to contact regarding this procurement process is:

The Chairman
BVI Ports Authority
Pasea Place
Road Town, Tortola VG1110
British Virgin Islands

Email address: jjthomas@bviports.org
Telephone: 1-284-294-3435 (ext. 2303) or 1-284-442-2290

2. BACKGROUND

2.1. The Ports Authority was established by the British Virgin Islands Ports Authority Act, No. 12 of 1990 (the Act), as a separate corporate entity, solely owned by the Government of the Virgin Islands. The mission of the Ports Authority is to provide superior quality seaport facilities and services, in an environment characterised by employee growth and development, cutting edge technology and teamwork for the betterment of the BVI. The Ports Authority is managed and directed by a Board of Directors. The primary responsibilities of the BVIPA are:

2.1.1. To carry out the day-to-day management and functions of all seaport facilities throughout the territory; inclusive of cargo, ferry and cruise ship.

2.2. The main objectives of this assignment are to:

2.2.1. Develop a framework for safeguarding Information Systems Assets and Resources;

2.2.2. Test the security of the BVIPA's existing IT infrastructure to identify risks and associated recommendations to mitigate the risks;

2.2.3. Develop a framework that allows for integrity, availability, and confidentiality of data;

2.2.4. Improve the Business Continuity Plan for the BVIPA; and

2.2.5. Improve system and operational efficiency at the BVIPA.

3. SCOPE OF SERVICES

3.1. The BVIPA is seeking the services of professional, experienced, competent, and resourceful firm (hereinafter referred to as the "Auditor") to conduct an Information Systems and Security Audit that will include ten (10) dimensions, more specifically defined below.

3.2. The Auditor shall conduct an **I. Information Systems Audit**, which will:

3.2.1. Assess the effectiveness of planning and oversight of IT activities;

3.2.2. Evaluate adequacy of operating processes and internal controls;

3.2.3. Assess the adequacy of Information Systems (IS), Information Technology (IT) policies and internal control procedures;

3.2.4. Identify areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions;

3.2.5. Assess whether the Information Security risks are appropriately identified and managed and whether the controls and risk management processes are adequate and implemented;

3.2.6. Examine the objectives of confidentiality, integrity and availability of data are maintained as per the requirement and the legal and regulatory requirements are complied with;

3.2.7. Examine the Information Systems resources are acquired economically, justifiably, used efficiently and protected adequately so as to effectively achieve the Port Authority's business objectives;

3.2.8. Assess the adequacy of Business Continuity Planning (BCP) arrangements with respect to periodical Vulnerability Assessment and Penetration Tests (VAPT) and corrective measures taken; and

3.2.9. Review all processes/systems using IT in any form, examine the level of compliance with the Ports Authority's current IT Policy and Information Security Policy.

3.3. The Auditor shall conduct an **II. IT General Controls Audit** to assess whether the data processing that takes place in systems and IT occurs in a controlled environment, supporting data integrity and security. More specifically, the IT General Controls Audit will include the following scope:

3.3.1. **Change Management** – To provide reasonable assurance that only appropriately authorized, tested, and approved changes are made to in-scope systems. The following attributes will be tested with appropriate evidence:

a) All changes are authorized, tested, approved and monitored;

b) Responsibilities are appropriately segregated; and

c) Procedures for Emergency changes.

3.3.2. **Logical Access Controls** – To assess that only authorized persons have access to data and applications (including programs, tables, and related resources) and that they can perform only specifically authorized functions. The following attributes will be tested with appropriate evidence:

a) General Security settings with respect to Application, Operating System and Database;

b) Privilege User Management;

c) Procedures for New User setup, Terminated Users, Transfers;

d) User Access Reviews

3.3.3. **Physical Access Controls** – To assess whether physical security controls are implemented in all areas where necessary, including video surveillance and door access.

3.3.4. **Environmental Controls** – To assess whether environmental controls are implemented in all areas, including air quality controls and fire safety measures.

3.4. The Auditor shall conduct a **III. General Process Audit**, which includes the following activities:

3.4.1. Assess the controls implemented in the system for: Input, Processing, Output and Functionality;

3.4.2. Review all types of Application Level Access Controls including proper controls for access logs and audit trails for ensuring Sufficiency & Security of Creation, Maintenance and Backup of the same. Only authorized users should be able to edit, input or update data in the applications or carry out activities as per their role and/or functional requirements;

3.4.3. Assess sufficiency & accuracy of event logging, adequacy of Audit trails, SQL command prompt usage, database level logging etc.;

3.4.4. Assess interface controls - Application interfaces with other applications and security in their data communication;

3.4.5. Assess authorization controls such as Maker Checker, Exceptions, Overriding exception & Error condition;

3.4.6. Assess Data integrity & File Continuity Controls;

3.4.7. Assess controls for user maintenance, password policies are being followed are as per Port Authority's IT& IS security policy with special attention to the use of hardcoded User ID & Password;

3.4.8. Review of all types of Parameter maintenance and controls implemented;

3.4.9. Assess controls for change management procedures including testing and documentation of change;

3.4.10. Identify gaps in the application security parameter setup in line with the Port Authority's security policies and leading best practices;

3.4.11. Audit of management controls including systems configuration/ parameterization & systems development;

3.4.12. Audit of controls over operations including communication network, data preparation and entry, production, file library, documentation and program library, Help Desk and

technical support, capacity planning and performance, Monitoring of outsourced operations;

3.4.13. Review of customizations done to the Software based on Port Authority's Policy followed for such customization;

3.4.14. Verify adherence to Legal and Statutory Requirements; and

3.4.15. Review of documentation for formal naming standards, design process of job roles, activity, groups, profiles, assignment, approval & periodic review of user profiles, assignment & use of Super user access.

Process Assessment - Authorization and Segregation of Duties Controls

3.4.16. Understand how system entitlements are used to enforce segregation of duties or authorized transactions;

3.4.17. Perform sample testing of user application entitlements to confirm appropriate segregations of duties are enforced by the system (in a test environment);

3.4.18. Perform sample testing of user application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel (in a test environment); and

3.4.19. Review of issue and findings log with the gaps/deviations/ issues noted (if any).

Process Assessment – Assessment of Role based Security for Applications under scope

3.4.20. Review of user creation, modification, deletion or maintenance procedures for the in-scope applications;

3.4.21. Review of privileged access rights granted to application, System Administrators and vendors;

3.4.22. Assess the process for review of user logs for administrator and system users;

3.4.23. Review ongoing monitoring of effectiveness of implemented procedures and controls;

3.4.24. Perform sample testing of application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel;

3.4.25. Review of account and password policy including controls such as users are assigned unique accounts;

3.4.26. Adequate passwords are maintained e.g. alphanumeric, minimum number of characters etc.;

3.4.27. Periodic password changes and preventing repeated use of passwords;

3.4.28. Review of implementation of password policy at system and application levels;

3.4.29. Account lockout policy for disabling user accounts after limited number of unsuccessful login attempts;

3.4.30. Review of Segregation of duties controls/ maker-checker controls through appropriate design and implementation of user roles / profiles;

3.4.31. Review how system entitlements are used to enforce segregation of duties or authorized transactions;

3.4.32. Perform testing of application's entitlements to confirm appropriate segregations of duties are enforced by the system (in a test environment);

3.4.33. Review how unsuccessful access attempts to applications in scope are logged and monitored;

3.4.34. Review the implementation and effectiveness of user access management in applications in the event of leaves; and

3.4.35. Review the segregation of development, production and test environments of applications.

3.5. The Auditor shall conduct a **IV. Data Governance Audit**, which will include the following scope:

3.5.1. Review of existing Data Classification;

3.5.2. Review how data is handled while being input, stored, manipulated, accessed, and deleted; and

3.5.3. Review loopholes from where data can be leaked.

3.6. The Auditor shall conduct a **V. Risk Management Assessment**, which will include:

3.6.1. Maintaining IT inventory

3.6.2. Classification of Assets

3.6.3. Classification of Information

3.6.4. Risk Assessment

3.6.5. Risk Treatment

3.6.6. Risk Mitigation

3.6.7. Residual Risks for which approval of appropriate authority should be obtained and;

3.6.8. The Risk Assessment is done periodically or whenever changes are made to IT infrastructure.

3.7. The Auditor shall conduct a **VI. Monitoring Audit**, which will assess:

3.7.1. Whether monitoring mechanism is adequate to prevent/ detect/ correct the security breaches if any, promptly;

3.7.2. Whether monitoring mechanism is capable to provide necessary alerts to stake holders and these alerts are acted upon;

3.7.3. Whether logs are pushed to a Central Syslog Server and these are secure from unauthorized access; and

3.7.4. Whether log analysis is not done by the same person whose actions are logged.

3.8. The Auditor shall conduct a **VII. Backup Management Audit**, which will determine:

3.8.1. Whether approved backup policy is in place and back up of data and software essential for the continued operations of the Ports Authority is taken as specified in the backup policy and such backups are tested periodically for recovery. The security controls over the backup data and media are stringent;

3.8.2. If the data supporting business information is properly backed-up so that it can be accurately and completely recovered if there is a system outage or data integrity issue. The following attributes needs to be tested with appropriate evidences:

a) Backup and Recovery

b) Job Scheduling

3.9. The Auditor shall conduct a **VIII. Disaster Recovery Audit,** which will assess:

3.9.1. Whether Disaster Recovery strategy adopted is adequate for continuity of operations of information systems which are critical to the Ports Authority's business in the event of disasters;

3.9.2. Whether it has necessary safeguards to minimize the risks, costs and duration of disruption to the business processes caused by disasters;

3.9.3. Whether Disaster Recovery Drills conducted were adequate enough to ensure continuity of operations in the event of actual disaster; and

3.9.4. If redundancy is configured for all critical applications including firewalls/ Routers and other network links and devices and work in times of contingency.

3.10. The Auditor shall conduct a **IX. Web Presence (Intranet & Internet) Audit,** to assess:

3.10.1. Whether the Ports Authority's websites and content management processes are in place to ensure that information published on these web sites is accurate, consistent and current;

3.10.2. If web browsing practices of employees are also as per the acceptable usage policy of the Port Authority and do not give scope to disrepute to the Ports Authority; and

3.10.3. If the Ports Authority's website maintenance is outsourced. The SP will have to review the SLA with the website maintenance vendor.

3.10.4. If IT Media handling is in compliance with the Port Authority's IT Policy;

3.11. The Auditor shall conduct a **X. Key IT Infrastructure Audit (Network Management and Security)**, which will include:

3.11.1. Hardening of computer systems, switches and routers and Firewalls;

3.11.2. Audit of Network design from security, integrity and availability point of view;

3.11.3. Audit of setting of Network equipment from security and functionality point of view;

3.11.4. Evaluation of Firewall policy and its implementation;

3.11.5. Review of appropriateness of the network topology;

3.11.6. Review of adequacy or otherwise of the hardware installed;

3.11.7. Key Applications Assessment (Internet Access, Anti-Virus, email, and document management, etc.).

4. DELIVERABLES

4.1. The deliverables for this consultancy include:

4.1.1. An Inception Report within 14 days of commencement of the contract that details, among other things, an updated work programme and method statement for delivering the consultancy;

4.1.2. A Draft Audit Report that encompasses the scope detailed in Sections 3.2 through 3.11 of this RFP, and contains observations on the gaps and shortcomings in the existing practices, with reference to best practices and industry standards. The Report should also contain the risks associated with non-adherence to best practices in the short, medium, and long-term, and recommendations for improvement (if any);

4.1.3. Presentation to the Board of Directors and any other staff of BVIPA, as required, on the findings of the assignment as documented in the Draft Audit Report; and

4.1.4. A Final Audit Report taking into consideration any feedback from the BVIPA on the Draft Audit Report prepared in 4.1.2.

5. PRE-TENDER MEETING

5.1. A virtual Pre-Tender meeting will be held via TEAMS on **Monday, 29th April 2024 at 9:00 am** (local time). The pretender meeting is not mandatory; however, it is recommended that each Tenderer attend. Each Tenderer must be fully informed regarding all existing and expected conditions and matters, which might affect the cost or performance of the Services. Any failure to fully assess the associated cost shall not relieve any Tenderer from responsibility to properly evaluate the difficulty or cost of successfully performing the Services.

6. SUBMISSION OF PROPOSALS

6.1. Tenderers will have two (2) options for submitting proposals before the date and time for submission of tenders.

6.2. **Option 1 – Hard Copy:** The Tenderer should submit one (1) original and three (3) copies of the Tender **no later than 4:00 p.m. (local time) on Thursday, 9 May 2024**. The original should be placed in a sealed envelope and marked "Original" and the copies placed in another sealed envelope and marked "Copy". Both envelopes should be placed in an outer envelope and marked **"RFP for Information Systems and Security Audit for British Virgin Islands Port Authority"**. The inner and outer envelope shall:

6.2.1. Be addressed to:

The Chairman
BVI Ports Authority
Pasea Place
Road Town, Tortola VG 1110
British Virgin Islands

6.2.2. Bear the following identification:

a) **"RFP for Information Systems and Security Audit for British Virgin Islands Port Authority"**

b) The words **"DO NOT OPEN BEFORE 10:00 am on 9 May 2024"**.

6.3. **Option 2 – Electronic Copy:** An electronic copy of the Technical Proposal and the Financial Proposal must be received **no later than 4:00 p.m. (local time) on 9 May 2024**. The submission must be in a non-editable format and not exceeding 10 MB. The body of the email submission should include the name and address of the tenderer and the subject of the email shall be **"RFP for Information Systems and Security Audit for British Virgin Islands Port Authority"**.

6.3.1. The electronic copy of the proposals must be submitted to the following address:

The Chairman
BVI Ports Authority
Pasea Place
Road Town, Tortola VG 1110
British Virgin Islands

Email: jjthomas@bviports.org

6.3.2. Bear the following identification:

a) **"RFP for Information Systems and Security Audit for British Virgin Islands Port Authority"**

b) The words **"DO NOT OPEN BEFORE 10:00 am on 9 May 2024"**.

6.4. It is the responsibility of the tenderer to ensure that the proposals are received by the Ports Authority before the aforementioned date and time for submission. **Late submissions will not be accepted**.

Documents Comprising Tender

6.5. Proposals must be submitted in accordance with paragraph 6.2 and 6.3 with documentary evidence (where applicable) that include the following:

6.5.1. General information on the tender as per attached **Form I: General Information**;

6.5.2. Letter of Confirmation as per attached **Form III: Letter of Confirmation**;

6.5.3. A list with brief descriptions of recent assignments that demonstrate a proven track record, solid reputation, success, and experience that are similar in scope to the requirements of this assignment that the firm has participated in as per attached **Form IV: Expertise and Experience**;

6.5.4. Organisation structure and curriculum vitae for the core team members that will be assigned to deliver the Services in accordance with **Form V: Profile of Audit Team** and **Form VI: Curriculum Vitae**;

6.5.5. Proposed audit approach and methodology for implementing the assignment;

6.5.6. Tenderers are required to submit a valid business licence or equivalency as proof of authorization to operate a business in the area of the required expertise in its jurisdiction of operation.

6.5.7. Tenderers registered in the BVI will be required to submit valid Certificates of Good Standing to the effect that the Tenderer has complied with the provisions and have fulfilled the obligations under the Social Security Act Ordinance, CAP. 266, Payroll Taxes Act No. 18. of 2004, Income Tax Ordinance CAP. 206 and National Health Insurance under the Social Security (Amendment) Act 2014 of the Laws of the Virgin Islands;

6.5.8. Tenderers registered in a jurisdiction outside of the BVI will be required to provide equivalent certifications that demonstrate that it is in good standing with respect to taxes and any other statutory obligations required in the jurisdiction of operation;

6.5.9. Executed Non-Disclosure Agreement as per attached **ANNEX C: Non-Disclosure Agreement**;

6.5.10. Form of Proposal as per attached **Form II: Form of Proposal**;

6.5.11. Completed cost proposal in accordance with **Form VII: Cost Proposal Questionnaire**

6.6. **The TECHNICAL PROPOSAL shall be comprised of documents required under 6.5.1 through 6.5.10**.

6.7. **The FINANCIAL PROPOSAL shall be comprised of documents required under 6.5.11 and 6.5.12**.

6.8. The Tenderer may wish to include any other documentary evidence to establish credentials.

7. EVALUATION OF TENDERS

7.1. The evaluation will be conducted three (3) stages: Preliminary Evaluation, Technical Evaluation and Financial Evaluation.

Preliminary Evaluation

7.2. The Preliminary Evaluation will include a pass/fail assessment of the following eligibility criteria:

7.2.1. The Tenderer must submit completed forms with details as per **Annex A and Annex C**;

7.2.2. The Tenderer must demonstrate that it has conducted at least three (3) Information Systems audits. Supporting information should be provided with **Form IV: Expertise and Experience**;

7.2.3. The Tenderer must demonstrate experience in conducting IT audits of Data Centres, Disaster Recovery Centres, Software Applications, Network Infrastructure, System

Security Evaluation and Computer System equipment assessment for three (3) years within the last five (5) years. Supporting information should be provided with **Form IV: Expertise and Experience**;

7.2.4. Tenderers registered in the BVI must have a valid trade licence, and must be in good standing with respects taxes owed to the Government, Social Security and National Insurance; and

7.2.5. Tenderers registered in a jurisdiction outside of the BVI must have a valid business licence, and must meet all statutory obligations in the jurisdiction of operation.

7.3. Only Tenderers that has substantially passed the Eligibility Criteria will be eligible for further evaluation in this RFP process.

Technical Evaluation

7.4. Technical Proposals for Tenderers passing the Eligibility Criteria will be evaluated in accordance with the following: The Technical Score will be conducted in accordance with the following criteria:

7.4.1. Qualifications of the Tenderer team members to undertake this assignment in accordance with **Form V: Profile of Audit Team** and **Form VI: Curriculum Vitae (25 points)**;

7.4.2. Demonstrated experience of the tenderer in performing similar assignments in accordance with **Form IV: Expertise and Experience (40 points)**;

7.4.3. Adequacy of proposed audit approach, work programme, and methodology for implementing the assignment **(30 points)**;

7.4.4. Any Tenderer demonstrating that is empaneled with CERT-In will be awarded **5 points** (empanelment certificate to be enclosed);

7.5. The maximum Technical Evaluation Score will be 100. **Only Tenderers achieving a Technical Score of 60 will be eligible for Financial Evaluation**.

Financial Evaluation

7.6. Financial Proposals for Tenderers passing the Eligibility Criteria, **and** achieving a Technical Score of 60, will be evaluated in accordance with the following:

7.6.1. Only the information provided on **Form VII: Cost Proposal Questionnaire** will be used to determine the Financial Score.

7.6.2. The maximum Financial Score will be **30**.

7.6.3. The Tender with the lowest evaluated the tender price will receive a Financial Score of 30. Financial Scores for all other Tender will be determined based on the following formula:

$$F = \frac{30 \times \mu}{Z}$$

where:

F = Financial Score for Tender being evaluated

μ = price of the lowest tendered Price

z = price of the Tender being evaluated

7.7. The Total Evaluation Score will be determined as the sum of the Technical Score and Financial Score. The Tenderer achieving the highest Total Evaluated Score will be selected as the preferred Tenderer, and will be invited to negotiate a contract to perform the Services.

8. OTHER CONDITIONS

8.1. The BVIPA reserves the right to accept or reject any or all proposals without assigning any reasons and is not obliged to correspond with the Applicants in this regard. Further, the BVIPA reserves the right to change and/or cancel the pre-qualification and tender process without assigning any reasons and without prejudice to its right to re-tender at any time in the future, and in such case no tenderer/intending tenderer shall have any claim arising out of such action.

8.2. The BVIPA reserves the right to invite revised responses from the Applicants by issue of an addendum, prior to the tender deadline, without liability or any obligation for such invitation and without assigning any reason. This RFP does not give rise to any rights and is not an offer or an invitation to offer.

8.3. The BVIPA, by this process, does not intend to assume any legal obligation whatsoever, including any binding relationship of any kind, with any Applicant, nor will the BVIPA accept any liability howsoever arising, in relation thereto. By this document, applicants are so informed, and unconditionally acknowledge that they are fully aware that through an invitation to submit proposals, no entitlement whatsoever vests, or will vest in them.

8.4. Participation by any party in this RFP pursuant to the invitation by the BVIPA shall be considered to be an acceptance of all the terms and conditions of this invitation by such party and no claims or disputes raised by it during or subsequent to the award process shall be entertained by the BVIPA.

8.5. All documents and other information supplied by the BVIPA or submitted by an Applicant to the BVIPA shall remain or become the property of the BVIPA. The BVIPA will not return any application or any information provided along therewith.

8.6. The applicants shall bear all costs associated with the preparation and submission of its Proposal. The BVPA will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the RFP process.

8.7. Proposals must be submitted in accordance with Section 6 of this RFP. The BVIPA shall not be responsible for the loss or non-receipt or delay in the receipt of any Proposals.

8.8. The address to be used for communication with BVIPA regarding this RFP is:

Board Secretary
BVI Ports Authority
Pasea Place
Road Town, Tortola VG 1110
British Virgin Islands
Tel: (1 284) 494-3435
Email: jjthomas@bviports.org

ANNEX A

TENDER FORMS

FORM I – GENERAL INFORMATION

Item	Tenderer's Information
Tenderer's name or registered name in the case of a firm:	
Tenderer's country of constitution	
Tenderer's year of constitution	
Tenderer's address or registered address (in the case of a firm) in the country of constitution	
Tenderer's authorized representative (name, address, telephone numbers, fax numbers, e-mail address)	
Is the Tenderer empaneled in CERT-In? *(If yes, please provide proof of certification.)*	☐ Yes ☐ No

Note:

- Please provide a certified true copy of the constitutional documents of the tenderer; e.g., business Licence, Company Registration, etc.

- Please provide board resolution/power of attorney in favor of authorized representative authorizing him/her submit the Proposal.

FORM II – FORM OF PROPOSAL

Date:

Chairman
BVI Ports Authority
Pasea Place
Road Town, Tortola VG1110
British Virgin Islands

REQUEST FOR PROPOSALS
"RFP for Information Systems and Security Audit for British Virgin Islands Port Authority"

Dear Chairman:

1. Based upon the Submission Requirements and the Scope of Services, the undersigned proposes to provide the Services as indicated in my RFP submission, and in accordance with the Tender Documents for the sum of (US$) (sum in words and figures)

_____

_____

payable by the British Virgin Islands Ports Authority (the "Employer").

2. The undersigned proposes to complete the assignment in _____ days and in accordance with the attached Schedule.

3. We agree that the proper law of the Contract shall be the Laws of the Virgin Islands.

4. We agree that these tender documents shall comprise the sole binding documentation applicable to this tender or to the contract.

5. We agree that all information supplied by the Employer to the Tenderer will be treated in confidence and not disclosed to third parties except insofar as this is necessary to obtain sureties or quotations for the purpose of submitting the tender. All information supplied by the Tenderer to the Employer will similarly be treated in confidence, except that references may be sought from banks, existing or past clients, or other referees submitted by the Tenderer.

6. We accept full responsibility for the accuracy of all prices provided in this tender and agree that these prices include full provision for any increases in the costs for whatsoever reason over the period of time from submission of tender to completion of the project and settlement of the final account.

7. We accept that any and all omissions or errors in pricing are our responsibility and agree that should any errors in arithmetic be discovered in the Cost Proposal submitted by us during consideration of this offer, these errors will be corrected by giving us an opportunity of either confirming our offer or amending it to correct such errors.

8. If this offer is accepted and subject to and in accordance with paragraphs 2, 3, 4, 5, 6, 7 above and the terms and conditions contained or referred to in the documents listed in paragraph 1, we undertake to provide the required services as in accordance with the contract.

Signed	.....
Name in BLOCK CAPITALS	.....
In the capacity of	.....
Duly authorized to sign tenders for and on behalf of:	
Name of Company	.....
Address	.....
.....	
Telephone No.	**Facsimile No.** .....

FORM III – LETTER OF CONFIRMATION

Date:

Chairman
BVI Ports Authority
Pasea Place
Road Town, Tortola VG1110
British Virgin Islands

REQUEST FOR PROPOSALS
"RFP for Information Systems and Security Audit for British Virgin Islands Port Authority"

Dear Chairman,

1. We confirm that we will abide by the conditions mentioned in this Request for Proposals (including Forms) in full and without any deviation subject to Forms.

2. We shall observe confidentiality of all the information passed on to us in course of the IS Audit process and shall not use the information for any other purpose than the current tender process.

3. We confirm that we have currently not been blacklisted by any Ministry, Department or agency of Government of the Virgin Islands, or a government in any other jurisdiction, or otherwise not involved in any such incident with any concern whatsoever, where the job undertaken or performed and conduct has been questioned by any authority, which may lead to legal action.

4. We confirm that we are not a vendor or consultant to the Ports Authority, and not involved in either the supply or installation of hardware or software, implementation of Security or Network Infrastructure of the Ports Authority, or providing services excluding IS Audit services, in the past three years directly or indirectly through a consortium.

Place:

Date: (Authorized Signatory)

SEAL

FORM IV – EXPERTISE AND EXPERIENCE

Provide details of the assignments where the Tenderer has performed IS audit of Data Centre, DRC, Operating Applications, or related Infrastructure for the Ports Authority or Other Organization during the past five (5) years as on the date of RFP.

Item No.	Client Name, Address, Representative and Phone No.	Description of Services	Location	Value	Start/ End dates	Notable Successes

Place:

Date: (Authorized Signatory)

SEAL

FORM V – PROFILE OF AUDIT TEAM

Enclose Individual curriculum vitae of each personnel assigned to deliver the Services under this assignment, in the format specified in **FORM VI**.

No.	Name	Role in this IS Audit (Task/Module)	Professional Qualification	Years of IS Audit Experience
1				
2				
3				
4				

Place:

Date: (Authorized Signatory)
SEAL

FORM VI – CURRICULAM VITAE

CV to be furnished on separate sheet for each member of the Core Audit team. Enclose proof of qualifications, experience, etc., as may be necessary.

DESCRIPTION	DETAILS
Name of the member	
Role of the Member	
Employee of the Audit Firm since:	
Designation:	
Educational Qualification:	
CISA certification Details:	
Other Certifications/accreditations: Total IS Audit Experience (no. of years, areas of experience) Experience in similar IS Audit Projects over the past three years member, activities performed, duration of experience)	

No.	Organization where the member was involved in IS Audit	Duration of involvement in months & year	Details of assignment done & role assigned

Place:

Date: (Authorized Signatory)
SEAL

FORM VII – COST PROPOSAL QUESTIONNAIRE

This questionnaire should be completed and submitted with the Proposal. **Completion of this questionnaire will form your Financial Proposal, which will be the ONLY price that will be evaluated**. **Providing a Financial Proposal in a format, other than this format, may result in a rejection of the Tender.**

	Component	Unit	Rate	Total
1	Direct Professional Fees[1]			
2	Reimbursable Expenses[2]			
Total Financial Proposal				

*The charge-out rates applicable to this consultancy are as follows:

Place:

Date: (Authorized Signatory)
SEAL

ANNEX B

[1] Include breakdown of Direct Professional Fees where applicable and necessary

[2] Include a breakdown for arriving at Reimbursable Expenses

AUDIT APPLICATION AND LOCATION DETAILS

Applications (includes but is not limited to:)

1. Core Operating Application
2. HR Applications
3. Ticketing Tool
4. Intranet
5. Website
6. Short Message Service (SMS) application
7. Dewy Decimal Classification Application
8. Biometric Application
9. Email Application

Locations

1. Head Office, Pasea Place (IT Operations)
2. Port Purcell (Container Port)
3. Road Town Jetty (Branch)
4. West End Ferry Terminal (Branch)
5. Dog Hole Jetty, Jost Van Dyke (Branch)
6. St. Thomas Bay, Virgin Gorda (Branch)
7. Gun Creek, Virgin Gorda (Branch)
8. Cyril B Romney Tortola Pier Park (Branch)

*More information is available on our website https:\\bviports.org

ANNEX C

NON-DISCLOSURE AGREEMENT

THIS RECIPROCAL NON-DISCLOSURE AGREEMENT (the "Agreement") is made in the British Virgin Islands between:

The Ports Authority constituted under the BVI Ports Authority Act as having its Corporate Office in Tortola, British Virgin Islands (hereinafter referred to as "the Ports Authority" which expression includes its successors and assigns) of the ONE PART;

AND

_____ (hereinafter referred to as " _____ " which expression shall unless repugnant to the subject or context thereof, shall mean and include its successors and permitted assigns) of the OTHER PART;

WHEREAS

- is carrying on business of providing _____ , has agreed to for the Ports Authority and other related tasks.

  _____

- For purposes of advancing their business relationship, the parties would need to disclose certain valuable confidential information to each other. Therefore, in consideration of covenants and agreements contained herein for the mutual disclosure of confidential information to each other, and intending to be legally bound, the parties agree to terms and conditions as set out hereunder.

NOW IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES AS UNDER

Confidential Information and Confidential Materials:

1. "Confidential Information" means non-public information that Disclosing Party designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential. "Confidential Information" includes, without limitation, information relating to installed or purchased Disclosing Party software or hardware products, the information relating to the general architecture of Disclosing Party's network, information relating to the nature and content of data stored within the network or in any other storage media, Disclosing Party's business policies, practices, methodology, policy design delivery, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to the Receiving Party by any Disclosing Party Subsidiary and/ or agents is covered by this agreement.

2. Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without Receiving Party's breach of any obligation owed to Disclosing Party; (ii) becomes known to Receiving Party prior to Disclosing Party's disclosure of such information to Receiving Party; became known to Receiving Party from a source other than Disclosing Party other than by the breach of an obligation of confidentiality owed to Disclosing Party; or (iv) is independently developed by Receiving Party.

3. "Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation written or printed documents and computer disks or tapes, whether machine or user readable.

Restrictions:

4. Each party shall treat as confidential the Contract and any and all information ("confidential information") obtained from the other pursuant to the Contract and shall not divulge such information to any person (except to such party's own employees and other persons and then only to those employees and persons who need to know the same) without the other party's written consent provided that this clause shall not extend to information which was rightfully in the possession of such party prior to the commencement of the negotiations leading to the Contract, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause). Receiving Party will have executed or shall execute appropriate written agreements with its employees and consultants specifically assigned and/or otherwise, sufficient to enable it to comply with all the provisions of this Agreement. If the Service Provider shall appoint any Sub-Contractor, then the Service Provider may disclose confidential information to such Sub-Contractor subject to such Sub Contractor giving the Ports Authority an undertaking in similar terms to the provisions of this clause.

5. Receiving Party may disclose Confidential Information in accordance with judicial or other ports related order to the intended recipients (as detailed in this clause), provided Receiving Party shall give Disclosing Party reasonable notice prior to such disclosure and shall comply with any applicable protective order or equivalent. The intended recipients for this purpose are:

    a. The statutory auditors of the Ports Authority and interested parties and deems it fit.
    b. Regulatory authorities regulating the affairs of the Ports Authority and inspectors and supervisory bodies thereof.

6. The foregoing obligations as to confidentiality shall survive any termination of this Agreement.

7. Confidential Information and Confidential Material may be disclosed, reproduced, summarized or distributed only in pursuance of Receiving Party's business relationship with Disclosing Party, and only as otherwise provided hereunder. Receiving Party agrees to segregate all such Confidential Material from the confidential material of others in order to prevent mixing.

8. Receiving Party may not reverse engineer, decompile or disassemble any software disclosed to Receiving Party.

Rights and Remedies:

9. Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized use or disclosure of Confidential Information and/ or Confidential Materials, or any other breach of this Agreement by Receiving Party, and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/ or Confidential Materials and prevent its further unauthorized use.

10. Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at Disclosing Party's request, or at Disclosing Party's option, certify destruction of the same.

11. Receiving Party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that Disclosing Party shall be entitled, without waiving any other rights or remedies (as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

    11.1 Suspension of access privileges

    11.2 Change of personnel assigned to the job

    11.3 Financial liability for actual, consequential or incidental damages

    11.4 Termination of contract

12 Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.

Miscellaneous:

13 All Confidential Information and Confidential Materials are and shall remain the property of Disclosing Party. By disclosing information to Receiving Party, Disclosing Party does not grant any expressed or implied right to Receiving Party to disclose information under the Disclosing Party patents, copyrights, trademarks, or trade secret information.

14 Any document provided under this Agreement is provided with RESTRICTED RIGHTS.

15 Neither party grants to the other party any license, by implication or otherwise, to use the Confidential Information, other than for the limited purpose of evaluating or advancing a business relationship between the parties, or any license rights whatsoever in any patent, copyright or other intellectual property rights pertaining to the Confidential Information.

16 The terms of Confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire product without use of the other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by person who has had access to the Confidential Information, including ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

17 This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequently to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party, its agents, or employees, except by an instrument in writing signed by an authorized officer of Disclosing Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

18 In case of any dispute, both the parties agree for neutral third-party arbitration. Such arbitrator will be jointly selected by the two parties and he/she may be an auditor, lawyer, consultant or any other person of trust. The said proceedings shall be conducted in the BVI Arbitration Center.

19 Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and assigns.

20 If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

21 All obligations created by this Agreement shall survive change or termination of the parties‟ business relationship.

Suggestions and Feedback:

22 Either party from time to time may provide suggestions, comments or other feedback to the other party with respect to Confidential Information provided originally by the other party (hereinafter “feedback”). Both parties agree that all Feedback is and shall be entirely voluntary and shall not in absence of separate agreement, create any confidentially obligation for the receiving party. However, the Receiving Party shall not disclose the source of any feedback without the providing party’s consent. Feedback shall be clearly designated as such and, except as otherwise provided herein, each party shall be free to disclose and use such Feedback as it sees fit, entirely without obligation of any kind to other party. The foregoing shall not, however, affect either party’s obligations hereunder with respect to Confidential Information of other party.

For and on behalf of

Name:

Designation:

Place:

Signature

For and on behalf of

Name:

Designation:

Place:

Signature: