Hong Kong Internet Registration Corporation Limited
香港互聯網註冊管理有限公司

Request for Proposals on Security Audit Services 2018

Version 1.0
Date: 8 August 2018

Hong Kong Internet Registration Corporation Limited

Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong.
Tel.: +852 2319 2303 Fax: +852 2319 2626
Email: info@hkirc.hk **Website:** www.hkirc.hk

IMPORTANT NOTICE

Table of Contents

1. Summary

HKIRC has been enhancing information security following the ISO/IEC 27001:2005 and ISO/IEC 27002:2005 standards. With reference to these international standards, an information security management system (ISMS) framework and a multitude of security controls and measures have been put into operation since 2007.

As part of the organization's strategy and commitment to foster information security, HKIRC is looking for a consultancy firm or IT security professional(s) ("the Contractor") to provide security audit services.

The Contractor selected by HKIRC will conduct an audit on the systems, network architectures, applications as well as the effectiveness of various implemented controls.

The Contractor shall conduct their audit independently with no influence on the auditing process by staff and directors. This arrangement will ensure high credibility of the security audit reports. The Contractor shall identify any design and operational gaps and provide feasible solutions with reference to established common good industry practice.

The required services are detailed in section 4 of this document.

Parties interested in providing this service shall submit **Expression of Interest (EOI)** by email to HKIRC proposal contacts listed under "Electronic Copy" in Appendix D **on or before 17 August 2018**.

For those who have submitted EOI, they should **submit proposal** to HKIRC **no later than 5:30pm on 3 September 2018**. The Tenderer must provide their information as required in the proposal cover page (Appendix D, section 1.3 Cover Page).

2. Definitions

The following terms are defined as in this section unless otherwise specified.

“Audit Committee” means the committee established by the HKIRC’s board of directors focusing on auditing matters. The committee members are drawn from members of the board of directors. The responsibilities of the committee are to 1) serve as a focal point for communication between other directors, the external auditors and the internal auditors as regards their duties relating to financial and other reporting, internal controls, external and internal audits for systems and operational processes and such other financial and accounting, systems and operational matters as the Board determines from time to time. 2) assist the Board in fulfilling its responsibilities by providing an independent review and supervision of financial reporting, systems and operational processes by satisfying themselves as to the effectiveness of the internal controls of the Company and its subsidiaries. Refer to https://www.hkirc.hk/pdf/TORAuditCommittee2007.pdf for details.

“The Contractor” means the company providing the Services.

“HKIRC” means Hong Kong Internet Registration Corporation Limited.

“HKDNR” means Hong Kong Domain Name Registration Company Limited, a wholly-owned subsidiary of HKIRC, the company requesting the proposal for “the Services”.

“ISMS” means Information Security Management System. It consists of an information security organization and a set of policies, guidelines and procedures concerned with information security management.

“RFP” means this Request for Proposal.

“The Services” means the consultancy services with requirements stipulated in Section 4 of this document.

“Tenderer” means the company who will submit proposal to provide the Services.

3. Background

3.1. About HKIRC

Hong Kong Internet Registration Corporation Limited (HKIRC) is a non-profit-distributing and non-statutory corporation responsible for the administration of Internet domain names under '.hk' and '.香港' country-code top level domains. HKIRC provides registration services through its registrars and its wholly-owned subsidiary, Hong Kong Domain Name Registration Company Limited (HKDNR), for domain names ending with '.com.hk', '.org.hk', '.gov.hk', '.edu.hk', '.net.hk', '.idv.hk', '.公司.香港', '.組織.香港', '.政府.香港', '.教育.香港', '.網絡.香港', '.個人.香港', '.hk' and '.香港'.

HKIRC endeavors to be:

- Cost-conscious but not profit-orientated
- Customer-orientated
- Non-discriminatory
- Efficient and effective
- Proactive and forward-looking

More information about HKIRC can be found at http://www.hkirc.hk .

HKIRC and HKDNR are listed as public bodies under the Prevention of Bribery Ordinance (Cap 201).

3.2. Current Environment Description

Details of the system, network infrastructure, applications, and their locations, will be provided to Tenderers who have submitted expression of interest and have signed both the Non-Disclosure Agreement (NDA) and the Information Security Compliance Statement (refer to section 5).

4. The Required Services

4.1. Project Objectives

The primary project objectives are to:

a. assess the security risks related to the use of information systems in HKIRC. The audit should not only focus on the information systems and data, but also on the security management aspect. The Contractor shall identify and recommend safeguards with the aim of strengthening the security controls to an acceptable level.

b. evaluate compliance with established security requirements [1] and the effectiveness of security controls being implemented; and

c. ensure that all identified risks have been mitigated or reduced to an acceptable level by performing a follow-up review.

4.2. Scope of Service

a. The following defines the scope of security audit service to be provided by the Contractor. The Tenderer can add or counter propose any tasks that they deem as necessary for completeness and effectiveness. Apart from the actual audit, a follow-up review on the audit findings is required for all items listed below.

b. There are 10 parts to the scope of service. Tenderers need to quote or propose for all parts. HKIRC reserves the right to take on all or any parts of the services. Tenderers are required to provide cost breakdown for each part. Refer to section 10(b).

c. Where applicable, both credentialed and non-credentialed vulnerability scanning should be performed. This requirement applies to all types of vulnerability scans or assessment stated below.

d. The Tenderer shall determine and state the percentage number of network equipment (4.2.2), hosts (4.2.2), wireless access point (4.2.3), database (4.2.4), applications (4.2.5) and workstations (4.2.6) they plan to cover during the audit in order to provide reasonable assurance over the security level of the respective population.

[1] Established security requirements in HKIRC are documented in: (i) *Information Security Policy*; (ii) *Information Security Guideline*; and (iii) *Information Security Classification Guideline*.

e. Tenderers shall explain their sampling approach in the methodology section of their proposal. In general, there is no need to sample the "non-production" assets, such as those being used for testing or development.

f. The number and type of scanning targets enumerated in (d) above will be disclosed to Tenderers in accordance with the pre-requisites outlined in section 3.2. The actual targets to be covered shall be mutually agreed between the Contractor and HKIRC.

4.2.1 System Architecture Design Review

Review the network and system architecture such as virtual machine infrastructure from a confidentiality, integrity and availability perspective. The review aims to find out if the architecture is capable of meeting HKIRC's business objectives and security objectives considering the infrastructure as a whole.

4.2.2 Network and Host Security Audit

The Contractor is required to carry out the following audits on the sampled network equipment and host systems. These include, but not limited to, firewall, router, switches, load balancers, IDS/IPS, NAS, physical hosts and virtual servers.

a. Perform internal vulnerability scanning and penetration testing to identify security weaknesses of network equipment and hosts from within the HKIRC internal network.

b. Perform external vulnerability scanning and penetration testing to identify security weaknesses of network equipment and hosts facing the Internet.

c. Evaluate the security settings of the network equipment and hosts against the company-wide security baselines or standards:

d. Use automated or manual techniques to examine the security settings and security rules of the network equipment and hosts to ensure that they are sufficiently protected from hackings and security attacks.

4.2.3 Wireless Network Security Audit

a. Discover rogue access points in the HKIRC office and the two data centers with access to HKIRC's infrastructure.

b. Perform vulnerability assessment on sampled, legitimate HKIRC wireless access points.

4.2.4 Database Security Audit

Review the security settings of sampled database servers. The audit aims to identify any database security issues and vulnerabilities.

4.2.5 Application Security Audit

a. Review the security settings of sampled applications, including their web servers and application servers. The audit aims to uncover the security control weaknesses of web-based applications.

b. Conduct external vulnerability scanning and penetration testing to identify security loopholes of sampled Internet-facing applications.

c. Perform internal vulnerability scanning and penetration testing to identify security loopholes of sampled web-based applications from within the HKIRC internal network.

4.2.6 Workstation Security Audit

a. Perform internal vulnerability scanning and penetration testing to identify security weaknesses of sampled workstations from within the HKIRC internal network.

b. Evaluate the security settings of the sampled workstations against the company-wide security baselines or standards:

c. Use automated or manual techniques to examine the security settings and configurations of sampled workstations to ensure that they are sufficiently protected from hackings and security attacks.

4.2.7 Data Backup and Recovery Audit

Review the current HKIRC data backup and recovery infrastructure and procedures. This should cover all kinds of routine backups, including, network equipment, hosts, database, file servers, emails, etc.

4.2.8 Audit on DDoS Impact

a. Review the existing DDoS mitigation mechanism, including the outsourced DDoS attack mitigation service, to determine:

i. whether the service levels[2] committed by HKIRC could be met under different types of DDoS attacks;

ii. the maximum size of various (types of) DDoS attacks that could be effectively handled by the existing infrastructure with nil or negligible service degradation.

b. Perform simulated DDoS attack service to test the effectiveness of the existing DDoS mitigation service. The simulation attack should be conducted in a manner *not* affecting the normal operation of HKIRC.

4.2.9 End User Awareness Audit

Test the security awareness of HKIRC's users by conducting a surprise mock phishing exercise.

4.2.10 DNSSEC Practice Statement (DPS) Audit

Perform audit on HKIRC DNSSEC environment conformities to the published DPS. This part should be conducted first during the audit fieldwork.

4.3. Deliverables

a. The Contractor shall develop and maintain a detailed project plan and arrange monthly progress meeting with HKIRC project team. Monthly progress report shall be delivered by the Contractor.

b. For each of the items above, HKIRC expect detailed description of the findings as well as the resolutions, including the corrective, preventive and detective measures applicable to HKIRC's production environment, in the form of one or more security audit reports.

c. Security audit report format and assessment severity classification:

i. All reported findings should be characterized by either of the following:

Host/ Device/ IP address	This includes all physical and virtual host as well as appliances and their operating system
System Applications	This includes any application that is not part of the operation system (either separately install or compile on the host)

[2] Official service level targets are published under: https://www.hkirc.hk/content.jsp?id=39

User Applications	Any application that is not part of the installed system application and is created specify for the company's business

ii. Four Assessment Severity Classifications shall be used in ranking the audit findings:

Critical	Issues that could compromise the significant internal control of the HKIRC, which might in turn, cause a direct or immediate adverse business / operational impact to HKIRC. Immediate attention by HKIRC was expected.
High	Issues that could compromise the important internal control of the HKIRC, which might in turn, cause a direct or adverse business / operational impact to HKIRC. In the short term, attention by HKIRC was expected.
Medium	Issues that could compromise the internal control of HKIRC, which might in turn, cause a possible adverse business / operational impact to HKIRC. These issues could be addressed in the medium term as there were other compensating controls established in HKIRC in addressing the identified risk or, at present, the risk exposure concerned is small, but this might not be the case if HKIRC business grows/changes.
Low	Issues that could compromise the internal control of HKIRC, which might not in turn cause a direct or adverse business / operational impact to HKIRC. Nevertheless, rectification of these issues would improve existing internal controls in the long-term, efficiency in HKIRC or ensure HKIRC followed current best practice in internal control.

iii. Item 4.2.10 above requires a separate audit report on its own. Other requirements shall be covered in a single security audit report.

d. A follow-up review report should be provided upon completion of the follow-up review for all the findings identified in section 4.2. Again, a separate follow-up review report is required for item 4.2.10.

e. The Contractor shall assist HKIRC in preparing the follow-up action plan which summarizes the action to be taken to address the recommendations.

f. A presentation to the management which summarizes the findings as well as the resolutions shall be conducted by the Contractor. Presentation slides are required.

g. The Contractor shall also provide one briefing session to the Audit Committee. The session aims to explain the security audit findings and resolutions. Presentation slides are required.

4.4. Minimizing Impact to Production Environment

a. Most of the vulnerability assessments and penetration tests will be performed against production environment. It is utmost important is to ensure all tests are non-destructive, non-intrusive and the influence on availability and performance of the production system are strictly minimized.

b. The times at which these tests are performed should be considered carefully, and well communicated to HKIRC.

c. The Contractor is required to disclose the actual tools to be used to conduct the audits.

d. Ensure that no malicious software (e.g. computer virus, worm, Trojan horse program), backdoor or anything which would disrupt the operation or lead to compromise of any system is embedded in either the information or its storage media (e.g. in the form of data file, database, document, program code, e-mail, floppy diskette, hard disk, CD-ROM, Internet web page) when they are disseminated and/or exchanged with HKIRC.

4.5. Project Management

a. The Contractor must assign a project manager who is responsible to develop the project plan, assign project tasks and quality related tasks, implementation of the plan, and ensure the overall quality of the project.

b. The project manager may adopt project management guides such as Project Management Institute (PMI)’s Project Management Body of Knowledge (PMBOK) Guide.

c. The project manager shall manage at least the following aspects of the project plus others as necessary: scope, time, cost, quality, human resources, communications, risk, procurement, integration and change control, information security and exception.

d. In particular, for communications, the Contractor shall provide regular project

status report and meeting (monthly) to the management.

4.6. Professional Staff Requirements

The Tenderer shall have at least five years of experience in providing similar security audit services. They shall provide recent references on **at least five** such projects in their proposal.

The Tenderer shall propose a project team, which consists of a project manager and **at least two** team members. The qualification, skills and experience of the project manager and members involved in the assignment should be provided in the proposal. The team MUST be full-time staff directly employed by the Tenderer. The requirements of the team are as follows:

a. The project manager should:
    1. possess at least 10 years of working experience in IT security; and
    2. have obtained CISA and/or CISSP qualification.

b. The team members should:
    1. possess at least 5 years of working experience in IT security; and
    2. have obtained CISA and/or CISSP qualification.

4.7. Service Location

The Services shall be provided in Hong Kong at all HKIRC's facilities including office and two data centers. The deliverables shall be delivered to the HKIRC's office.

5. Information Security

a. The Tenderer shall acknowledge and agree that, if the Tenderer is selected as the Contractor, it shall be bounded by our Non-Disclosure Agreement (NDA) and the HKIRC Information Security Policy. The Contractor shall also comply with the obligations under the Personal Data (Privacy) Ordinance and any other obligations in relation to personal data.

b. The Tenderer shall be provided with a set of NDA and Information Security Compliance Statement after HKIRC received the company's Expression-of-Interest before the stipulated time. The NDA and the Information Security Compliance Statement shall be signed and returned to HKIRC attached with documents required by the Compliance Statement before the scheduled deadline. **HKIRC will only consider proposals from companies which have signed both the NDA and the Information Security Compliance Statement.**

c. The proposal should be marked "RESTRICTED" at the centre-top of each page in black color. It must be encrypted if transmitted electronically.

d. Each proposal will be reviewed under the terms of non-disclosure by the HKIRC's staff and Board of Directors of HKIRC.

e. The Contractor shall comply with the following HKIRC security policy and guidelines, to the extent that commensurate with its roles and responsibilities. The term "Contractor" hereby refers to all relevant staff members of Contractor and those of any other subcontractors under the Contractor's purview.

   i. Information Security Policy;

   ii. Information Security Guideline; and

   iii. Information Security Classification Guideline.

f. Contractor's Information Security Policy is subject to HKIRC review if needed.

6. Anti-collusion

a. The Tenderer shall not communicate to any person other than HKIRC the amount of any tender, adjust the amount of any tender by arrangement with any other person, make any arrangement with any other person about whether or not he or that other person should or should not tender or otherwise collude with any other person in any manner whatsoever in the tendering process. Any breach of or non-compliance with this sub-clause by the Tenderer shall, without affecting the Tenderer's liability for such breach rules and laws or non-compliance, invalidate his tender.

b. Sub-clause (a) of this section shall have no application to the Tenderer's communications in strict confidence with his own insurers or brokers to obtain an insurance quotation for computation of tender price and communications in strict confidence with his consultants/sub-contractors to solicit their assistance in preparation of tender submission.

c. The Tenderer shall submit to the HKIRC a duly signed warranty in the form set out in Appendix B to the effect that he understands and will abide by these clauses. The warranty shall be signed by a person authorized to sign the contract on the Tenderer's behalf.

d. Any breach of any of the representations and/or warranties by the Tenderer may prejudice the Tenderer's future standing as a HKIRC's contractor.

7. Offering Advantages

a. The Tenderer shall not, and shall procure that his employees, agents and sub-contractors shall not, offer an advantage as defined in the Prevention of Bribery Ordinance, (Cap 201) in connection with the tendering and execution of this contract.

b. Failure to so procure or any act of offering advantage referred to in (1) above committed by the Tenderer or by an employee, agent or sub-contractor of the Tenderer shall, without affecting the Tenderer's liability for such failure and act, result in his tender being invalidated.

8. Ethical Commitment

8.1. Prevention of bribery

a. The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, except with permission of Hong Kong Internet Registration Corporation Limited (hereafter referred to as the Organization) solicit or accept any advantage as defined in the Prevention of Bribery Ordinance (Cap 201) in relation to the business of the Organization. The Contractor shall also caution his directors, employees, agents and sub-contractors against soliciting or accepting any excessive hospitality, entertainment or inducements which would impair their impartiality in relation to the business of the Organization. The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors are aware of the aforesaid prohibition and will not, except with permission of the Organization, solicit or accept any advantage, excessive hospitality, etc. in relation to the business of the Organization.

b. The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, offer any advantage to any Board member or staff in relation to the business of the Organization.

8.2. Declaration of Interest

c. The Contractor shall require his directors and employees to declare in writing to the Organization any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract. In the event that such conflict or potential conflict is disclosed in a declaration, the Contractor shall forthwith take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed. The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

d. The Contractor shall prohibit his directors and employees who are involved in this Contract from engaging in any work or employment other than in the performance of this Contract, with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests

and their duties in connection with this Contract. The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

e. The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors who are involved in this Contract are aware of the provisions under the aforesaid sub-clauses (c) and (d).

8.3. Handling of confidential information

f. The Contractor shall not use or divulge, except for the purpose of this Contract, any information provided by the Organization in the Contract or in any subsequent correspondence or documentation, or any information obtained when conducting business under this Contract. Any disclosure to any person or agent or sub-contractor for the purpose of the Contract shall be in strict confidence and shall be on a "need to know" basis and extend only so far as may be necessary for the purpose of this Contract. The Contractor shall take all necessary measures (by way of internal guidelines or contractual provisions where appropriate) to ensure that information is not divulged for purposes other than that of this Contract by such person, agent or sub-contractor. The Contractor shall indemnify and keep indemnified the Organization against all loss, liabilities, damages, costs, legal costs, professional and other expenses of any nature whatsoever the Organization may suffer, sustain or incur, whether direct or consequential, arising out of or in connection with any breach of the aforesaid non-disclosure provision by the Contractor or his directors, employees, agents or sub-contractors.

8.4. Declaration of ethical commitment

g. The Contractor shall submit a signed declaration in a form (see Appendix C) prescribed or approved by the Organization to confirm compliance with the provisions in aforesaid sub-clauses (a), (b), (c), (d), (e) and (f) on prevention of bribery, declaration of interest and confidentiality. If the Contractor fails to submit the declaration as required, the Organization shall be entitled to withhold payment until such declaration is submitted and the Contractor shall not be entitled to interest in that period. To demonstrate compliance with the aforesaid sub-clauses (a), (b), (c), (d), (e) and (f) on prevention of bribery, declaration of interest and handling of confidential information, the Contractor and the

sub-contractors employed for the performance of duties under this Contract are required to deposit with the Organization a copy of the internal guidelines issued to their staff.

9. Project Schedule

The tentative project schedule is proposed below. Contractors should strive to complete the audit in around three months' time. Nevertheless, interested Tenderers may propose an alternative project plan in the event that the tentative schedule below is deemed infeasible or subject to high-degree of uncertainty.

	Project Schedule Tasks	*Required Completion Date*	*Deliverables*
	Stage 0: Selection & Appointment of Contractor		
1.	Publish Request for Proposal (RFP)	10/08/2018	
2.	Submit Expression of interest	17/08/2018	
3.	Sign NDA and Information Security Compliance Statement with all interested Tenderers	17/08/2018	
4.	Deadline for Tenderers to submit proposal and quotation	03/09/2018 5:30 pm	
5.	Selection of Contractor by panel	17/09/2018	
6.	Conclude final decision and appoint the Contractor	22/10/2018	
7.	Prepare service agreement	29/10/2018	
8.	Sign service agreement with the appointed Contractor	05/11/2018	
	Stage 1: Project Initiation		
9.	Prepare detailed project plan	05/11/2018	Detailed project plan
10.	Formation of project organization	12/11/2018	
11.	Project initiation meeting	12/11/2018	
	Stage 2: Implementation		
12.	Conduct all reviews listed under section 4.2	31/12/2018	
13.	Draft security audit report and DPS audit report (refer to 4.3(c)(iii))	15/01/2019	
14.	Conduct presentation to report the findings to senior management.	31/01/2019	Presentation slides
15.	Finalize security audit report and DPS audit report	15/02/2019	Security Audit

	Project Schedule Tasks	*Required Completion Date*	*Deliverables*
			Report; DPS Audit Report
16.	Prepare follow-up action plan (jointly by the Contractor and HKIRC)	15/03/2019	Follow-up Action Plan
17.	Conduct briefing to Audit Committee	March 2019	Presentation slides
	Stage 3: Follow-up Review		
18.	Conduct follow-up review on all findings[1]	14/06/2019	
19.	Draft follow-up review report	28/06/2019	
20.	Finalize follow-up review report	15/07/2019	Follow-up Review Report
	Stage 4: Project Closing		
21.	Return or destroy of all information or documents given to Contractor for audit purpose	31/07/2019	

Notes:

1. The follow-up review is scheduled to commence around five months from the fieldwork completion date of the audit (step 12). The exact timing will be agreed with the Contractor in due course.

10. Payment Schedule

a. The proposal shall be submitted on the basis of "fixed lump sum" for providing the required services in conformity with this RFP.

b. Interested Tenderers shall provide the breakdown of the cost, in Hong Kong Dollars, **of all required service** specified under section 4.2.

c. The Tenderers should make certain that prices quote are accurate before submitting their proposal. Under no circumstances will the HKIRC accept any request for adjustment on the grounds that a mistake has been made in the proposed prices.

d. The following payment schedule is recommended but interested Tenderers may propose their own in their proposals.

	Milestone/Acceptance of Deliverables	**Payment %**
1	Acceptance of detailed project plan	10%
2	Acceptance of security audit reports and DPS audit report (refer to section 4.2.10)	70%
3	Acceptance of follow-up review reports	20%
	TOTAL	**100%**

11. Service Acceptance

The overall service acceptance can be broken down into acceptances at various levels:-

a. Services provided and their quality
b. Deliverables and their quality
c. Overall quality of the project/service

Under this acceptance framework, the Contractor should fulfill the Scope of Services described in section 4.2. Interested Tenderers may provide additional acceptance criteria and the related plan in detail in their proposals.

12. Service Agreement Negotiation and Signature

The service agreement will be drawn up **between the selected Contractor and HKDNR**, the wholly-owned subsidiary of HKIRC. HKIRC welcomes the Tenderer's proposal on a suitable service agreement for the project/service.

The service agreement must be signed by both parties within two week from the project/service award date. If the agreement is not signed within the said period, HKIRC will start the negotiation with the next qualified Tenderer on the selection list.

13. Elements of a Strong Proposal

All submitted proposal must following the format as stated in Appendix D - HKIRC Proposal Requirements.

Appendix A – HKIRC Contacts

HKIRC Contacts information

Contacts	
Hong Kong Internet Registration Corporation Limited Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong +852 23192303 – telephone +852 23192626 – fax http://www.hkirc.hk *If you are not sure about the appropriate person to call, the receptionist can help you.*	**Information Security Manager** Ken WONG +852 23193822 ken.wong@hkirc.hk **Head of IT** Ben LEE +852 23193811 ben.lee@hkirc.hk **Deputy CEO** Bonnie CHUN +852 23193808 bonnie.chun@hkirc.hk

Appendix B – Warranty

To: Hong Kong Internet Registration Corporation Limited (HKIRC)

Dear Sir/Madam,

Warranty

(1) By submitting a tender, the Tenderer represents and warrants that in relation to the tender of Security Audit Services:

(i). it has not communicated and will not communicate to any person other than the HKIRC the amount of any tender price;

(ii). it has not fixed and will not fix the amount of any tender price by arrangement with any person;

(iii). it has not made and will not make any arrangement with any person as to whether it or that other person will or will not submit a tender; and

(iv). it has not otherwise colluded and will not otherwise collude with any person in any manner whatsoever in the tendering process.

(2) In the event that the Tenderer is in breach of any of the representations and/or warranties in Clause (1) above, the HKIRC shall be entitled to, without compensation to any person or liability on the part of the HKIRC:

(i). reject the tender;

(ii). if the HKIRC has accepted the tender, withdraw its acceptance of the tender; and

(iii). if the HKIRC has entered into the contract with the Tenderer, terminate the contract.

(3) The Tenderer shall indemnify and keep indemnified the HKIRC against all losses, damages, costs or expenses arising out of or in relation to any breach of any of the representations and/or warranties in Clause (1) above.

(4) Clause (1) shall have no application to the Tenderer's communications in strict confidence with its own insurers or brokers to obtain an insurance quotation for computation of the tender price, or with its professional advisers, and consultants or sub-contractors to solicit their assistance in preparation of tender submission. For the avoidance of doubt, the making of a bid by a bidder to the HKIRC in public during an auction will not by itself be regarded as a breach of the

representation and warranty in Clause (1)(i) above.

(5) The rights of HKIRC under Clauses (2) to (4) above are in addition to and without prejudice to any other rights or remedies available to it against the Tenderer.

Authorized Signature & Company Chop :

Name of Person Authorized to Sign (in Block Letters) :

Name of Tenderer in English (in Block Letters) :

Date :

Appendix C – Declaration Form by Contractor on their Compliance with the Ethical Commitment Requirements

To: Hong Kong Internet Registration Corporation Limited (HKIRC)
Contract No.: _____
Title: _**Security Audit Service 2018**_____

In accordance with the Ethical Commitment clauses in the Contract:

1) We confirm that we have complied with the following provisions and have ensured that our directors, employees, agents and sub-contractors are aware of the following provisions:

   a) prohibiting our directors, employees, agents and sub-contractors who are involved in this Contract from offering, soliciting or accepting any advantage as defined in section 2 of the Prevention of Bribery Ordinance (Cap 201) in relation to the business of HKIRC except with the permission of HKIRC;

   b) requiring our directors, employees, agents and sub-contractors who are involved in this Contract to declare in writing to their respective company management any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract, and in the event that a conflict or potential conflict is disclosed, take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed;

   c) prohibiting our directors and employees who are involved in this Contract from engaging in any work or employment (other than in the performance of this Contract), with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract and requiring our agents and sub-contractors to do the same; and

   d) taking all measures as necessary to protect any confidential/privileged information or data entrusted to us by or on behalf of HKIRC from being divulged to a third party other than those allowed in this Contract.

Signature
(Name of the Contractor)
(Name of the Signatory)
(Position of the Signatory)
(Date)

Appendix D – HKIRC Proposal Requirements

Proposal requirements	
Submission deadline	Please refer to Section 9 – Project Schedule, item no. 4 for the proposal submission deadline. If tropical cyclone warning signal No.8 or above or the black rainstorm warning is hoisted on the deadline date, the deadline will be postponed to the next working day without advance notice.
Delivery address	Hong Kong Internet Registration Corporation Limited Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong
Hard copies	Sending hard copies is not mandatory. For sending hard copies, 2 copies of the full proposal are required. The proposal shall be sent to the attention of Elisa CHUNG (Senior Finance Officer) or Peon LIU (HR & Admin Manager).
Electronic copy	Electronic copy is mandatory. It shall be sent by email to elisa.chung@hkirc.hk and peon.liu@hkirc.hk; also cc ken.wong@hkirc.hk and ben.lee@hkirc.hk.
Proposal format	Specified in this document
Page count	30 pages or fewer. Stapled. Do not bind.
Font	Electronically published or typed. Times New Roman 12 point font.

Successful Tenderer is the one who submitted a clearly worded proposal that demonstrates the following attributes:

- a persuasive section on the company background
- international recognize certification for security audit
- a strong and flexible service and tools meeting HKIRC requirements with minimum customization
- high level of interaction between HKIRC and the Contractor
- excellent fit with the capabilities and facilities of HKIRC
- strong company and project management team

1.1 Proposal Deadline

All proposals must reach HKIRC as stated in Section 9, Project Schedule, item no. 4.

1.2 Proposal Content

The proposal should contain the following:

- Cover Page
- Executive Summary
- Conflict of Interest Declaration
- Company Background
    - Financial Situation
    - Track Records
    - Organization and management team
    - Project team with credentials
    - Company credentials
    - Staff credentials
- Methodology
- Project management methodology
- Understanding of our requirements
- Knowledge and Advices on Projects/Services
- Deliverable and Services level
- Proposed Cost of Services and Payment Schedule
- Implementation Time Table
- Commercial and Payment Terms. e.g. Compensation for delay.

1.3 Cover Page

Prepare a non-confidential cover page with the following information in the order given.

Cover Page		
Project Title		
		Security Audit Service 2018
Project Manager	Name:	
	Title:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
Company	Contact person:	
	Title:	
	Company name:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
	Website:	

1.4 Executive Summary

The executive summary provides a brief synopsis of the commercial and technical solution the Tenderer proposed for the project/service. This summary must be non-confidential. It should fit on a single page.

The executive summary should be constructed to reflect the merits of the proposal and its feasibility. It should also clearly specify the project/service's goals and resource requirements. It should include:

- Rationale for pursuing the project or service, the methodology/technology needed and the present state of the relevant methodology/technology.
- Brief description of the Tenderer's financial situation.
- Brief description of the Tenderer's facilities and experience on similar projects or services

1.5 Conflict of Interest Declaration

Declare any conflict of interest in relation to the project and the '.hk' ccTLD registry HKIRC.

1.6 Company Background

The Tenderer must describe its company background. Major activities, financial situation, organizational structure, management team and achievements in similar projects/services or service outsourcing of the company should be elaborated. Track records are preferred.

List the key technical and management personnel in the proposal. Provide a summary of the qualifications and role of each key member.

1.7 Methodology

The Tenderer must describe the methods to be used, and briefly explains its advantage and disadvantage. Track records are preferred.

1.8 Project Management Methodology

The Tenderer must describe the methods to be used, and briefly explains its advantage and disadvantage. Track records are preferred.

1.9 Understanding of our requirements

The Tenderer shall describe their understanding of our requirements. With the use of a table, the Tenderer should clearly state their compliance on the requirements listed in the scope of service section; and briefly explain how they are achieved.

1.10 Knowledge and Advices on Projects/Services

The Tenderer should describe their knowledge and advices to ensure the success of this project/service or projects/services with similar nature.

1.11 Deliverable and Services level

The Tenderer should detail the project/service deliverables, and the services level of the proposed services. **Tables of content of all reports included in the deliverables should be provided in the proposal**.

1.12 Proposed Costs of Service and Payment Schedule

The Tenderer should provide the breakdown of the cost of the whole project/service. The cost shall be broken down by milestone/phases. The payment shall be scheduled based on the milestones and/or deliverables.

Such costs should include, if applicable:

- Fixed setup cost
- Labour unit costs for additional services or requirements. They are typically quoted in unit man day. Quoted in normal working hour, non-working hour and in emergency.
- Equipment that is permanently placed or purchased for HKIRC to complete the project or service, if any.
- Subsequent support, maintenance or consultation service.
- Other direct costs including services, materials, supplies, postage, traveling, pocket money, etc.

1.13 Implementation Time Table

The Tenderer should present in this section the implementation schedule of the project/service. The schedule should be realistic and achievable by the Tenderer.

1.14 Commercial and Payment Terms

The Tenderer should describe the commercial and payment terms of the services e.g. compensation for the delay of the project/service.