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

Version 1.0
Date: 25 April 2017

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 is looking for an auditing firm or IT security audit professional(s) ("the Contractor") to provide the security audit services.

HKIRC has been enhancing information security following the ISO27001:2005 and ISO27002:2005 standards. In December 2007, HKIRC have realized an ISMS framework and have planned or implemented security controls and measures in operation.

The Contractor selected by HKIRC will conduct an audit/assessment on the systems and network architectures as well as the effectiveness of various implemented controls by 29 September 2017.

The Contractor shall conduct their audit/assessment 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 scope of service is detailed in section 4 of this document.

Parties interested in providing this service shall submit **Expression of Interest (EOI) by 12 May 2017**. For those who have submitted EOI, they should **submit proposal** (see Appendix D) to the Group **no later than 5:30pm on 2 June 2017**.

The Contractor should submit Expression of Interest by email to HKIRC contacts (refer to Appendix D - HKIRC Proposal Requirements, electronic copy). The Contractor must provide their information as required in the proposal cover page (Appendix D, 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.

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

“RFP” means this Request for Proposal

3. 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 endeavours 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 .

4. The Required Services

4.1. Scope of Service

The following defines the scope of security audit service to be provided by the Contractor

The vendor can add or counter propose any tasks that they deem as necessary for completeness and effectiveness.

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

4.1.1 System architecture design review

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

4.1.2 External network/firewall vulnerability assessment

- Perform network based security scans to identify security weaknesses of components supporting the critical IT infrastructure.
- Baseline review
    - Network baseline
        - Firewall, router, switches and loadbalancer configuration, IDS/IPS etc.
    - Host System baseline, both virtual and physical.
- External (Internet facing) Vulnerability Assessment
    - Network Vulnerability Assessment includes all Internet services provided by HKIRC.
    - Application Vulnerability Assessment

4.1.3 External penetration test to web applications

- Conduct penetration tests to identify security holes of web applications.

4.1.4 Router, firewall and switch review/assessment

- Use automated or manual techniques to check security settings of the routers,

firewalls and switches to ensure that they are sufficiently protected from hackings and security attacks.

4.1.5 Application security review/assessment

- Review the security settings of applications. The review aims to uncover the security control weaknesses of the major.
- Service should include Application Vulnerability Assessment

4.1.6 Database server review/assessment

- Review the security settings of database servers. The review aims to identify any database security issues.
- Service should include Database Vulnerability Assessment

4.1.7 Internal vulnerability scanning – operating systems

- Check and identify any vulnerability in the operating systems. The check aims to identify any vulnerability that can be exploited with access to the server being tested.

4.1.8 Internal penetration test – network services

- Check and identify any vulnerability in the operating systems. The check aims to identify any vulnerability that can be exploited through other machines within the local network and not externally reachable.

4.1.9 Wireless network assessment

- Check and identify any unauthorized wireless access point.
- Check for rogue access point at Data Centre for assess to HKIRC's infrastructure.
- Vulnerability Assessment of all HKIRC wireless access points.

4.1.10 Data Backup and Recovery assessment

- Audit the current HKIRC Data Backup and Recovery infrastructure and procedures.

4.1.11 Assessment on DDOS impact

- Check and identify any impacts from Distributed Denial of Service (DDOS) attacks based on network bandwidth resources. The check aims to identify the impacts by different types of DDOS attacks on the ability of our systems and network infrastructure to provide the intended services with the committed service levels, and the maximum traffic of the different types of DDOS attacks that our infrastructure can handle with no or different extents of service degradation.

- Service should also include DDOS Attack mitigation Assessment

Optional:

- As an optional service, vendor can propose 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.

4.1.12 DNSSEC Practice Statement (DPS) Audit

- Vendor should perform audit on HKIRC DNSSEC environment conformities to the publish DPS.

4.1.13 End User Awareness

Optional:

- Vendor can propose service to test the security awareness of HKIRC's users. This could be in form of a simulated phishing email attack.

4.2. Deliverables

- For each of the items above, HKIRC expect detailed reports detailing the findings as well as the resolutions, including the corrective, preventive and detective measures applicable to HKIRC's production environment.
- A briefing session to the management which summarize the findings as well as the resolutions.
- Security Report Format and Assessment Severity Classification

All reported assessment severity count should be based on either of the following:

1) Host/Device/IP address – This includes all physical and virtual host as well as appliances and their operating system.
2) System Applications – This includes any application that is not part of the operation system (either separately install or compile on the host).
3) User Applications – Any application that is not part of the installed system application and is created specify for the company's business.

Four Assessment Severity Classifications shall be use:

1) 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.

2) 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.
3) 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.
4) 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.

Three types of report are required:

1. Host Based Summary report count should be based on the highest severity on each host, if the host has more than one issue. An aggregate % of each of the Severity Classification over total number of audited host shall be presented in the report.

2. Application Based Summary (System and User) report count should be based on the highest severity on each application, if the application has more than one issue. An aggregate % of each of the Severity Classification over total number of audited application shall be presented in the report.

3. Issue Based Summary report count should be based on catalog of issues identified and included all application and host audited. This will be used for issue tracking and action planning purposes.

4.3. Disclosure of the tools used

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

4.4. Minimizing impact to production environment

- Most of the infrastructure 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.
- The times at which these tests are performed should be considered carefully, and well communicated to HKIRC.

4.5. Table of contents and additional deliverables

- The vendor must provide the tables of contents of the deliverables in the proposal.
- The vendor may propose addition deliverables if considered appropriate.

4.6. Information security

- The Contractor shall follow HKDNR Information Security Policy and Guidelines set out by HKDNR on personal and co-operation data security.
- Contractor's Information Security Policy is subject to HKIRC review if needed.

4.7. Project management

This service is expected to be delivered over a period of 3 months. Its success is highly dependent on the management of the project.

- 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
- The project manager may adopt project management guides such as PMI's PMBOK.
- The project manager shall manage at least the below aspects of the project plus others as necessary
    1. Scope
    2. Time
    3. Cost
    4. Quality
    5. HR
    6. Communications
    7. Risk
    8. Procurement
    9. Integration and Change Control
    10. Information Security
    11. Exception
- In particular, for communications, the Contractor shall provide regular project status report and meeting (monthly) to the management.
- The Contractor shall provide one (1) briefing session to the Audit Committee. The session aims to explain the security audit findings and resolutions.

4.8. Service Acceptance

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

1. Services provided and their quality
2. Deliverables and their quality
3. Overall quality of the project/service

Under this acceptance framework, the vendor should fulfill the scope of services described in section 4.1. Interested vendors may provide additional acceptance criteria and the related plan in detail in their proposals.

4.9. Service Location

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

5. Information Security

The company submitting the proposal ("the company") shall acknowledge and agree that, if the company is selected as the Contractor, it shall be bounded by our Non-Disclosure Agreement (NDA) and Information Security Policy (highlights of the policies are illustrated in Appendix A). The company shall also comply with the obligations under the Personal Data (Privacy) Ordinance and any other obligations in relation to personal data.

The company 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.**

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

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

6. Anti-collusion

(1) 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.

(2) Sub-clause (1) of this Clause 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.

(3) 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.

(4) 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

(1) 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.

(2) 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 Organisation) solicit or accept any advantage as defined in the Prevention of Bribery Ordinance (Cap 201) in relation to the business of the Organisation. 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 Organisation. 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 Organisation, solicit or accept any advantage, excessive hospitality, etc. in relation to the business of the Organisation.

(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 Organisation.

8.2. Declaration of Interest

(C) The Contractor shall require his directors and employees to declare in writing to the Organisation 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 Organisation 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 Organisation against all loss, liabilities, damages, costs, legal costs, professional and other expenses of any nature whatsoever the Organisation 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 Organisation 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 Organisation 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 Organisation a copy of the internal guidelines issued to their staff.

9. Project Schedule

	Project Schedule Tasks	*To be Completed by*	*Remark*
1	Publish RFP	5/5/2017	
2	Expression of interest	12/5/2017	
3	Sign NDA and InfoSec Compliance Statement with all interested vendors	12/5/2017	
4	Deadline for vendors to submit proposal and quotation	2/6/2017, 5:30pm	
5	Selection of vendor by panel	12/6/2017	
6	Conclude final decision and appoint the vendor	28/6/2017	
7	Prepare service agreement	7/7/2017	
8	Sign service agreement with the appointed vendor	14/7/2017	
9	Security Audit complete with deliverables	6/10/2017	

10. Payment Schedule

Interested vendors shall provide the breakdown of the cost, in Hong Kong Dollars, of the whole service specified in the proposal.

The Contractors 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.

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

	Milestone/Acceptance of Security Audit	**Payment %**
1	Upfront payment at start	30%
2	Acceptance of deliverables	60%
3	Completion of the overall project/service	10%
	TOTAL	**100%**

11. Elements of a Strong Proposal

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

12. Service Agreement Negotiation and Signature

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

The service agreement must be signed by both parties within one 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 vendor on the selection list.

13. 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 23191313 – telephone +852 23192626 – fax http://www.hkirc.hk *If you are not sure about the appropriate person to call, the receptionist can help you.*	**IT Project Manager** Ben Choy +852 23193819 ben.choy@hkirc.hk **Head of IT** Ben Lee +852 23193811 ben.lee@hkirc.hk **CEO** Leo Lam +852 23193821 leo.lam@hkirc.hk

Appendix A – HKDNR Information Security Policy and Guidelines: An Extract Relevant to Outsourcing

This document provides an extract of the HKDNR Information Security Policy and Guidelines with the purposes of (a) introducing various measures and controls to be executed by HKDNR regarding outsourcing and (b) setting the expectation of any potential contractors that their participation and conformance in these measures and controls are essential contractual obligations.

The original Policy and Guidelines applies to HKDNR's employees, contractors and third party users. However, a potential contractor may interpret the clauses up to their roles and responsibilities only. Nonetheless, the keyword "**contractors**" hereby refers to all relevant staff members of the contractor and those of any other subcontractors under the contractor's purview.

Herein, HKDNR would also set the expectation of any potential contractors that upon their expression-of-interest to the project/service, they shall be required in the subsequent stages (a) to sign off a non-disclosure agreement (NDA) on all information to be provided and (b) to sign off a Compliance Statement where compliance requirements are specified in more details.

(A) Extract from the HKDNR Information Security Policy

In the following, "the organization" means Hong Kong Domain Name Registration Company Limited, the company requesting the proposal for "the Project."

8. Human resources security

8.1 Security objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

8.1.1 Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.

8.1.2 Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

8.1.3 As part of their contractual obligations, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.

8.2 During employment
Security objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

8.2.1 Management shall require employees, contractors and third party users to apply security measures in accordance with established policies and procedures of the organization.

8.2.2 All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates on organizational policies and procedures, as relevant to their job functions.

8.3 Termination or change of employment
Security objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

8.3.2 All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

8.3.3 The access rights of all employees, contractors and third party users to information and information processing facilities shall either be removed upon termination of their employment, contract or agreement, or adjusted upon change.

12. Information systems acquisition, development and maintenance
12.5.5 Outsourced software development shall be supervised and monitored by the organization

13. Information security incident management

13.1 Reporting information security events and weaknesses

Security objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action.

13.1.2 All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

(B) Extract from the HKDNR Information Security Guidelines

6. ORGANIZING INFORMATION SECURITY

6.2 EXTERNAL PARTIES

6.2.1 Identification of Risks Related to External Parties

The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting the access.

6.2.3 Addressing Security in Third Party Agreements

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

7. ASSET MANAGMENT

7.1.3 Acceptable Use of Assets

Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

8. HUMAN RESOURCE SECURITY

8.1.1 Roles and Responsibilities

Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.

8.1.2 Screening

Background verification checks on all candidates for employment, contractors, and third party users shall be conducted in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

8.1.3 Terms and Conditions of Employment

As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.

8.2.1 Management Responsibilities

Management shall require employees, contractors and third party users to apply security measures in accordance with established policies and procedures of the organization.

12. Information systems acquisition, development and maintenance

12.5.5 Outsourced Software Development

Outsourced software development shall be supervised and monitored by the organization.

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:

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	2 copies of the full proposal are required. The proposal shall be to the attention of Elisa Chung (Finance Officer)
Electronic copy	Electronic copy, if available, on disk or by email to elisa.chung@hkirc.hk and bonnie.chun@hkirc.hk; also cc ben.choy@hkirc.hk and ben.lee@hkirc.hk. This is not a substitute for the physical copies mentioned above.
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 vendor 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 vendor
- 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 Services
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 vendor 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 vendor's financial situation.
- Brief description of the vendor'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 vendor 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 vendor must describe the methods to be used, and briefly explains its advantage and disadvantage. Track records are preferred.

1.8 Project Management Methodology

The vendor 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 vendor shall describe their understanding of our requirements. With the use of a table, the vendor 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 vendor 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 vendor 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 vendor 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 vendor should present in this section the implementation schedule of the project/service. The schedule should be realistic and achievable by the vendor.

1.14 Commercial and Payment Terms

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