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

Request for Proposals on ISO 27001 Consultancy Service

Version 2.0
Date: 5 June 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 professional services leading to certification under the ISO 27001 standard.

The Contractor shall provide expert advice and assistance to HKIRC to revamp the existing ISMS and implement a "fit-for-purpose" ISMS based on the latest version of the ISO 27001 standard.

In addition, the Contractor appointed by HKIRC shall provide an onsite internal audit (aka pre-assessment) service to determine the readiness of HKIRC for the initial assessment to certification scheduled to commence by the end of 2018.

Lastly, the Contractor shall provide onsite advisory and support to HKIRC throughout the course of formal assessment to be conducted by a Certification Body.

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 11 June 2018**. For those who have submitted EOI, they should **submit proposal** (see Appendix D) to the Group **no later than 5:30pm on 25 June 2018**.

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.

“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.

“ISO 27001” means the latest version of the international standard ISO/IEC 27001. At the time of writing this RFP, the latest version is 2013.

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

“RFP” means this Request for Proposal.

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

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 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).

4. The Required Services

4.1. Background

HKIRC provides the administration of Internet domain names under '.hk' and .香港 country-code top level domains. Domain Name Registration services provided by HKIRC included the following:

- Domain name resolution for country-code top level domains names under '.hk' and .香港
- Domain name register for country-code top level domains names under '.hk' and .香港
- WHOIS service for country-code top level domains names under '.hk' and .香港

HKIRC has about 30 full time staff of which 12 are under IT Department. In collaboration with external service providers, the IT Department is responsible for managing and supporting the IT infrastructure located at two data center facilities and one office in Hong Kong.

4.2. Scope of Service

The proposal shall be submitted on the basis of "Fixed Lump Sum" for providing the required services in conformity with this RFP. The project objective is to:

a. provide expert advice and assistance to HKIRC to revamp the existing ISMS and implement a "fit-for-purpose" ISMS based on the latest version of the ISO 27001 standard;
b. provide an onsite internal audit service to determine the readiness of HKIRC for the initial assessment to certification; and
c. provide onsite advisory and support to HKIRC throughout the course of formal assessment to ensure a smooth assessment process.

The tentative subject of certification and ISMS scope statement for the purpose of ISO 27001 certification are stated below for your reference:

Subject: HKIRC and its wholly owned subsidiary HKDNR

Scope statement: IT services and operations in support of the provisioning of domain name registration services

It is the intention of HKIRC to limit the scope of this project to the IT Department and its operations, with minimal involvement of other departments in the organization. The final wording of the subject and scope statement is subject to change where necessary.

4.2.1 Proposed Services

There are three parts to the required services. Vendor needs to quote/propose for all parts. HKIRC reserves the right take on all or any parts of the services.

4.2.1.1. Part A: Consultancy Service

The proposed services should include, but not limited to, the followings:

a. Identification and validation of the gaps with respect to ISO 27001;
b. Implementation of measures and controls to close the gaps identified and validated with respect to ISO 27001. Specifically it will include:
    1. Revamp of the existing Information Security Management System (ISMS);
    2. Conducting a risk assessment, developing and implementing a treatment plan;
    3. Development of the necessary documentation based on HKIRC's requirements and input. A list of mandatory and commonly used documentations to be delivered are enclosed in Appendix E; and
    4. Preparation of ISO 27001 scope statement and Statement of Applicability (SOA).
c. Providing ISO 27001 ISMS training to HKIRC staff within the ISMS scope.

4.2.1.2. Part B: Internal Audit Service

Prior the official assessment to certification, an onsite internal audit (aka pre-assessment) service should be performed to determine the readiness of the in-scope services for the formal assessment. Activities during the onsite internal audit should include, but not limited to, the following:

a. Assess the prepared ISMS and activities conducted by the relevant teams;
b. Benchmark against the ISO 27001 standard and identify any non-conformity (NC); and
c. Provide assistance and support to HKIRC on remediating all non-conformities, including the revision of all necessary documentations.

4.2.1.3. Part C: Onsite Support during Formal Assessment

The Contractor should provide onsite advisory and support throughout the course of formal assessment to be conducted by a Certification Body. This should include, but not limited to, the following:

a. Attend interviews and site-visits with the external assessors;
b. Assist in the identification and collection of audit evidence; and
c. Follow up on queries raised by the Certification Body.

4.2.2 Project Timeframe

HKIRC intends to obtain ISO 27001 certification by end of February 2019. Please refer to section 9 for detailed project schedule.

4.2.3 Project Management Requirements

The Contractor is responsible for project management of the proposed service. The duties of project management will include the following:

a. Responsibility for the total project management and act as a single contact point to HKIRC regarding all related activities of the project;
b. Take the lead in coordinating various parties within and outside HKIRC for the smooth implementation of the project;
c. Resolve conflicts and crisis during the entire project life cycle;
d. Oversee and monitor the progress of various activities during the project life cycle to ensure that these activities are completed according to the implementation schedule and meeting the project requirements;
e. Plan and schedule meetings at appropriate time during the project life cycle, to

prepare meeting agenda, to chair and to take notes for all the meetings with various parties;

f. Report progress, follow up all outstanding issues with all related parties, suggest solutions and resolve difficulties throughout the project; and
g. Any other activities which are necessary for the satisfactory completion of the project.

4.2.4 Competence of Consultants

The Contractor shall have at least five years of experience in providing similar consultancy service. They shall provide recent references on at least two such projects leading to ISO 27001 certification in their proposal.

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

a. The team leader should:
    1. possess at least 10 years of working experience in IT security;
    2. possess at least 10 years of solid working experience in ISO 27001 audit or implementation, preferably with non-profit organizations; and
    3. have obtained Lead Auditor or Lead Implementer qualification on ISO 27001 standard

b. The team members should:
    1. possess at least 5 years of working experience in IT security;
    2. possess at least 5 years of solid working experience in ISO 27001 audit or implementation; and
    3. have obtained Lead Auditor or Lead Implementer qualification on ISO 27001 standard

4.3. 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 vendor should fulfill the Scope of Services described in section 4.2. Interested vendors may provide additional acceptance criteria and the related plan in detail in their proposals.

4.4. 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

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

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 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.

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 meet the target date for ISO 27001 certification stated under task 20. Nevertheless, interested vendors 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	*To be Completed by*	*Deliverables*
	Tender Invitation and Award		
1	Publish RFP	06/06/2018	
2	Expression of interest	11/06/2018	Signed Expression of Interest
3	Sign NDA and InfoSec Compliance Statement with all interested vendors	19/06/2018	Signed NDA & compliance statement
4	Deadline for vendors to submit proposal and quotation	25/06/2018 5:30 pm	Proposal and quotation
5	Selection of vendor by panel	09/07/2018	
6	Conclude final decision and appoint the vendor	23/07/2018	
7	Prepare service agreement	30/07/2018	
8	Sign service agreement with the appointed vendor	06/08/2018	Signed service agreement
	Project Initiation		
9	Prepare detailed project plan	10/08/2018	Detailed project plan
10	Formation of project organization	10/08/2018	
11	Project initiation meeting	13/08/2018	
	Part A: Consultancy Service		
12	Identification and validation of gaps with respect to ISO 27001	13/09/2018	Gap Analysis Report

	Project Schedule Tasks	*To be Completed by*	*Deliverables*
13	Implementation of measures and controls to close the gaps identified and validated	15/11/2018	All documents listed under Appendix E.
14	Provisioning of ISO 27001 ISMS training to HKIRC staff	15/11/2018	Training materials
	Part B: Internal Audit Service		
15	Assess the prepared ISMS and related activities	30/11/2018	
16	Benchmark against the ISO 27001 standard and identify any non-conformity	30/11/2018	Internal Audit report
17	Provide assistance and support to HKIRC on remediating all non-conformities	31/12/2018	Depends on internal audit results
	Part C: Onsite Support during Formal Assessment		
18	Initial assessment*	31/01/2019	Per request from assessor
19	Certification application	31/01/2019	
20	ISO 27001 Certified	**28/02/2019**	

* Tasks 18~20 are supposed to be performed by a Certification Body to be engaged separately. The Contractor is required to provide onsite advisory and support to HKIRC throughout the formal assessment period (task 18).

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 Deliverables	**Payment %**
Part A: Consultancy Service		
1	Delivery and acceptance of the gaps analysis report	20%
2	Implementation of measures and controls to close the gaps identified and validated with respect to ISO 27001	70%
3	Provision of ISO 27001 ISMS training to HKIRC staff within the ISMS scope	10%
	TOTAL	**100%**
Part B: Internal Audit Service		
1	Delivery and acceptance of the internal audit report	40%
2	Completed remediation of all non-conformities identified during internal audit	60%
	TOTAL	**100%**
Part C: Onsite Support during Formal Assessment		
1	Provision of onsite advisory and support to HKIRC during the assessment period.	100%
	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.*	**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 23193821 bonnie.chun@hkirc.hk

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

This document provides an extract of the HKIRC Information Security Policy and Guidelines with the purposes of (a) introducing various measures and controls to be executed by HKIRC 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 HKIRC'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, HKIRC 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 HKIRC 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 HKIRC 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: Request for Proposals on ISO 27001 Consultancy Service

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 (Finance Officer) or Kris LAM (Executive Officer).
Electronic copy	Electronic copy is mandatory. It shall be sent by email to elisa.chung@hkirc.hk and kris.lam@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 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		
		ISO 27001 Consultancy 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.

Appendix E – List of Mandatory Documentations Required by ISO 27001

The list below shows the minimum set of documents required by ISO 27001. Items marked as "non-mandatory" are not mandatory per ISO standard but they are very often used. It is recommended that these items are also included in the deliverables.

No.	Documents*	ISO 27001:2013 clause number
1.	Acceptable use of assets	A.8.1.3
2.	Access control policy	A.9.1.1
3.	Backup policy (Non-mandatory)	A.12.3.1
4.	Bring your own device (BYOD) policy (Non-mandatory)	A.6.2.1
5.	Business continuity procedures	A.17.1.2
6.	Business continuity strategy (Non-mandatory)	A.17.2.1
7.	Business impact analysis (Non-mandatory)	A.17.1.1
8.	Change management policy (Non-mandatory)	A.12.1.2, A.14.2.4
9.	Clear desk and clear screen policy (Non-mandatory)	A.11.2.9
10.	Controls for managing records (Non-mandatory)	7.5
11.	Definition of security roles and responsibilities	A.7.1.2, A.13.2.4
12.	Disposal and destruction policy (Non-mandatory)	A.8.3.2, A.11.2.7
13.	Exercising and testing plan (Non-mandatory)	A.17.1.3
14.	Incident management procedure	A.16.1.5
15.	Information classification policy (Non-mandatory)	A.8.2.1, A.8.2.2, A.8.2.3
16.	Information security policy and objectives	5.2, 6.2
17.	Information transfer policy (Non-mandatory)	A.13.2.1, A.13.2.2, A.13.2.3
18.	Inventory of assets	A.8.1.1
19.	Legal, regulatory, and contractual requirements	A.18.1.1
20.	Maintenance and review plan (Non-mandatory)	A.17.1.3
21.	Mobile device and teleworking policy	A.6.2.1

	(Non-mandatory)	
22.	Operating procedures for IT management	A.12.1.1
23.	Password policy (Non-mandatory)	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
24.	Procedure for corrective action (Non-mandatory)	10.1
25.	Procedure for document control (Non-mandatory)	7.5
26.	Procedure for internal audit (Non-mandatory)	9.2
27.	Procedures for working in secure areas (Non-mandatory)	A.11.1.5
28.	Risk assessment and risk treatment methodology	6.1.2
29.	Risk assessment and risk treatment report	8.2, 8.3
30.	Risk treatment plan	6.1.3 e), 6.2
31.	Scope of the ISMS	4.3
32.	Secure system engineering principles	A.14.2.5
33.	Statement of Applicability	6.1.3 d)
34.	Supplier security policy	A.15.1.1