HONG KONG INTERNET REGISTRATION CORPORATION LTD.

HONG KONG DOMAIN NAME REGISTRATION COMPANY LTD.

REQUEST FOR PROPOSAL ON SECURITY AUDIT SERVICE 2026-2028

Version 1.4

SEP 2025

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

This communication contains information which is confidential and may also be privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any distribution, copying or use of this communication or the information in it is strictly prohibited. If you have received this communication in error, please notify the sender immediately and then destroy any copies of it.

Table of Content

1. SUMMARY 1
2. DEFINITIONS 3
3. BACKGROUND 4
4. THE REQUIRED SERVICES 5
5. INFORMATION SECURITY 16
6. ANTI-COLLUSION 17
7. OFFERING ADVANTAGES 17
8. COMPLIANCE WITH LAW 18
9. ETHICAL COMMITMENT 18
10. PROJECT SCHEDULE 21
11. ENGAGEMENT OPTIONS & PAYMENT SCHEDULE 22
12. SERVICE ACCEPTANCE 23
13. SERVICE AGREEMENT NEGOTIATION AND SIGNATURE 23
14. ELEMENTS OF A STRONG PROPOSAL 23
APPENDIX A – HKIRC CONTACTS 24
APPENDIX B – WARRANTY 25
APPENDIX C – DECLARATION OF ETHICAL COMMITMENT 27
APPENDIX D – HKIRC PROPOSAL REQUIREMENTS 28

1. SUMMARY

1.1 HKIRC has been enhancing information security by making reference to the ISO/IEC 27001 standard since 2007. In April 2019, HKIRC achieved certification in the ISO/IEC 27001:2013 standard to demonstrate its commitment to information security. With reference to this international standard, an information security management system (ISMS) framework and a multitude of security controls and measures have been put into operation since 2007.

1.2 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 service.

1.3 The Contractor selected by HKIRC will conduct an audit on, among others, the high-level system architecture, servers, network, databases, applications, workstations, Wi-Fi, as well as the effectiveness of the existing DDoS mitigation service and data backup strategy. It is also responsible for conducting a mock phishing test and a DNSSEC Practice Statement Audit. The required services are detailed in section 4.2 of this document.

1.4 This tender comprises three annual security audit services over a period of three years starting mid-2026.

1.5 The Contractor shall conduct their audit independently with no influence on the auditing process by staff and directors of HKIRC. 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 industry best practice.

1.6 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 23 September 2025.

1.7 For those who have submitted EOI, they should submit proposal to HKIRC no later than 5:30 pm on 30 September 2025. The Tenderer must provide their information as requested in the proposal cover page (see APPENDIX D).

1.8 Tenderers will be invited to a presentation after submission of proposal. Timeline for the vendor invitation, proposal presentation, evaluation and appointment process are summarized in the table below for your reference. HKIRC reserves the right to adjust the schedule as it sees appropriate.

Step	Description	Tentative date
1	Issue Request for Proposal (RFP)	16 SEP 2025
2	Tenderers to submit Expression of Interest (EOI)	23 SEP 2025
3	Sign NDA with interested Tenderers	23 SEP 2025
4 *	Deadline for Tenderers to submit proposal	30 SEP 2025
5	Proposal presentation, tenderer evaluation, and recommendation by HKIRC Selection Panel	OCT~NOV 2025
6	Approve Contractor by Audit Committee or the Board	9 NOV 2025
7	Initiate and clear internal procurement procedures	31 DEC 2025
8	Sign service agreement with Contractor	JAN 2026

2. DEFINITIONS

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

Audit	The terms "audit" and "assessment" are used interchangeably in this RFP. "Audit" in the context of this document has no connection whatsoever to the statutory audits or financial audits imposed by laws or regulations.
Audit Committee	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.
Contractor	The company providing the Services requested in this RFP.
HKIRC	Hong Kong Internet Registration Corporation Limited. It is the company requesting proposal for the Services.
HKDNR	Hong Kong Domain Name Registration Company Limited, a wholly owned subsidiary of HKIRC.
HKMA	Hong Kong Monetary Authority
ISMS	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	Request for Proposal
Services	The consultancy services with requirements stipulated in section 4 of this document.
Tenderer	The company who will submit proposal to provide the Services.

3. BACKGROUND

3.1 ABOUT HKIRC

3.1.1 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'.

3.1.2 HKIRC and HKDNR endeavor to be:

(a) Cost-conscious but not profit-orientated

(b) Customer-orientated

(c) Non-discriminatory

(d) Efficient and effective

(e) Proactive and forward-looking

3.1.3 More information about HKIRC and HKDNR can be found at https://www.hkirc.hk and https://www.hkdnr.hk respectively.

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

3.2 CURRENT ENVIRONMENT DESCRIPTION

3.2.1 Number and type of servers, network equipment, databases, applications, workstations and Wi-Fi access points, will be provided to Tenderers who have submitted expression of interest and have signed the Non-Disclosure Agreement (NDA) for the sole purpose of fee estimation under this RFP by the Tenderer.

4. THE REQUIRED SERVICES

4.1 PROJECT OBJECTIVES

4.1.1 The primary project objectives are to:

(a) assess the technical security risks related to the configuration of information systems in HKIRC[1]. The Contractor shall identify and recommend safeguards with the aim of strengthening the security configuration to an acceptable level;

(b) evaluate compliance with HKIRC information security policies and standards, as well as 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.

4.1.2 The audit period to be covered for items 4.2.1 to 4.2.9 and 4.2.11 is from 1 July 2025 to 31 March 2026 for the first-year audit; from 1 April 2026 to 31 March 2027 for the second-year audit; and from 1 April 2027 to 31 March 2028 for the third year.

4.1.3 For item 4.2.10 (DNSSEC Practice Statement Audit in the first and third year), the audit period is from 1 April 2026 to 31 March 2027 for the first year and from 1 April 2027 to 31 March 2028 for the third year.

4.2 SCOPE OF SERVICE

The following defines the scope of security audit service to be provided by the Contractor. Apart from the actual audit, a **follow-up review** of the audit findings is required for all items listed below.

(a) There are ten mandatory components within the scope of services (Session 4.2.1 to 4.2.10) and one optional component (Session 4.2.11). Tenderers are required to quote for all mandatory components. HKIRC reserves the right to select any or all components of the services. Tenderers must provide a detailed cost breakdown for each component. For further details, please refer to Section 11.4.

(b) Both credentialed and non-credentialed vulnerability scanning should be performed. This requirement applies to all types of vulnerability scans outlined in the sub-sections below.

[1] Both HKIRC and HKDNR share the same IT infrastructure and staff resources. The audit objectives, scope and deliverables are expected to cover both companies.

(c) The auditor shall cover ALL servers, network equipment, databases, applications, workstations, Wi-Fi access points in both production and non-production environment that came to their attention during vulnerability scanning and penetration testing. In other words, the sampling rate is 100%. In scope device are listed as follow:

No.	Systems	No. of servers	Location	Usage
1	DNRS2	16	Primary DC	Production Servers
2	DNRS2	16	Secondary DC	Production Servers
3	HKIRC Website	2	Primary DC	Production Servers
4	HKIRC Website	2	Secondary DC	Production Servers
5	HKIRC Website	4	Primary DC	Network & Security Device
6	HKIRC Website	4	Secondary DC	Network & Security Device
7	HKDNR Website	3	Primary DC	Production Servers
8	HKDNR Website	3	Secondary DC	Production Servers
9	HKDNR Website	4	Primary DC	Network & Security Device
10	HKDNR Website	4	Secondary DC	Network & Security Device
11	Backup System	3	Primary DC	Production Servers
12	Backup System	4	Primary DC	Network & Security Device
13	Backup System	4	Secondary DC	Network & Security Device
14	Internal IT Service	1	Primary DC	Production Servers
15	Internal IT Service	1	Secondary DC	Production Servers
16	Internal IT Service	1	Office	Production Servers
17	Internal IT Service	8	Primary DC	Network & Security Device
18	Internal IT Service	8	Secondary DC	Network & Security Device
19	Internal IT Service	5	Office	Network & Security Device
20	Multiable Accounting System	2	Primary DC	Production Servers
21	Multiable Accounting System	2	Secondary DC	Production Servers
22	Multiable HR	2	Primary DC	Production Servers
23	Multiable HR	2	Secondary DC	Production Servers

4.2.1 System Architecture Design Review

(a) Review the network and system architecture such as virtual machine infrastructure from a confidentiality, integrity and availability perspective. The review aims to find out whether there are significant loopholes or design flaws in the existing infrastructure at a high-level.

(b) Review the security of our Office 365 services, including Outlook 365, OneDrive, SharePoint, Azure Virtual Desktop (AVD), etc. Focus should be on the risk of data leakage and unauthorized access to sensitive data.

(c) Review the design and effectiveness of the existing vulnerability management procedures.

(d) Review the lifecycle management process of (i) privileged user accounts and (ii) general Windows AD user accounts. Sample checking shall be done to verify the effectiveness of the related security measures, including but not limited to, the approval and granting of admin rights to IT staff. The Contractor is required to outline the sampling criteria in their proposal.

(e) Review of governance of IT security.

4.2.2 Server and Network Security Audit

(a) The Contractor is required to carry out the following assessments on all servers and network equipment. These include, but not limited to, firewall, router, switches, load balancers, IDS/IPS, NAS, storage appliances, physical servers, virtual servers, and IoT devices.

(b) Perform internal vulnerability scanning and penetration testing to identify security weaknesses of servers and network equipment from within the HKIRC internal network and remotely via SSLVPN and AVD with (i) a general user account and (ii) a IT user account using (A) company-provided notebook and (B) privately-owned computing equipment.

(c) Perform external vulnerability scanning and penetration testing to identify security weaknesses of all servers and network equipment facing the Internet.

(d) Evaluate the security settings of all servers and network equipment against the company-wide security standards and baselines.

(e) Use automated or manual techniques to examine the security settings and security rules of all servers and network equipment to ensure that they are sufficiently protected from hackings and security attacks.

4.2.3 Database Security Audit

(a) Review the security settings of all database servers with an aim to identifying any database security issues, misconfigurations, and vulnerabilities.

(b) Review the adequacy of data protection and privacy measures in place to safeguard personal data stored in all databases against data leakage and unauthorized access.

4.2.4 Application Security Audit

(a) Review the security settings of all applications, including their web servers and application servers. The audit aims to uncover the security control weaknesses of web-based applications by referring to some recognized security standards or benchmarks, such as OWASP Top 10 Web Application Vulnerabilities and OWASP Top 10 API Vulnerabilities, as proposed by the Contractor.

(b) Perform internal vulnerability scanning and penetration testing to identify security loopholes of all web-based applications from within the HKIRC internal network.

(c) Conduct external vulnerability scanning and penetration testing to identify security loopholes of all Internet-facing applications.

4.2.5 Workstation Security Audit

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

(b) Evaluate the security settings of all workstations against the company-wide security standards and baselines.

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

(d) Review the adequacy of end-point protection measures to thwart ransomware and intentional/unintentional data leakage by internal staff from (i) IT department; and (ii) non-IT department.

4.2.6 Wireless Network Security Audit

(a) Discover rogue access points within the HKIRC office.

(b) Perform vulnerability scanning on all legitimate HKIRC wireless access points.

4.2.7 Audit on DDoS Impact

(a) Review the existing DDoS mitigation service agreement to determine whether there is sufficient protection to safeguard the HKIRC network against common:

(i) volumetric attacks;

(ii) protocol attacks; and

(iii) application layer attacks

based on the prevailing trend in DDoS at the time of the audit.

(b) Perform a mock DDoS attack to test the readiness of the DDoS mitigation service provider and internal staff in responding and handling such attacks. The simulation attack should be conducted in a manner not affecting the normal operation of HKIRC.

(c) Review the large-scale 'simulated DDoS attack' performed by HKIRC to stress-test the ability of the current DDoS mitigation service to withstand modern-day DDoS attacks.

4.2.8 Data Backup and Recovery Audit

(a) Review the current HKIRC data backup and recovery strategy and procedures. This shall cover all kinds of routine backups configured in servers, network equipment, databases, file servers, NAS, storage appliances, Office 365 services, etc.

(b) Review the disaster recovery mechanism for dual-site failure scenario and the associated drill records.

(c) Review the disaster recovery policy, procedures, and relevant drill records to determine the coverage and effectiveness of the existing disaster recovery program, readiness of staff in responding to catastrophic system failures, and compliance to internal security policies.

4.2.9 End User Awareness Audit

(a) Test the security awareness of HKIRC's users by conducting a simulated mock phishing exercise on all incumbent staff.

(b) Deliver a one-hour security awareness training to all staff with a short quiz at the end to reinforce their understanding of the key points. Contractor is required to prepare the training materials and quiz questions.

(c) Review the "customer awareness and education" related measures by referring to section 4.3 of Supervisory Policy Manual on Risk Management of E-banking (TM-E-1) published by the HKMA. Such measures should include the provision of regular security advice to .hk registrants, guidelines and training to customer service officers, monitoring and removal of fake or suspicious websites or apps, as well as emergency notification to customers and/or general public in the event of such incidents.

4.2.10 DNSSEC Practice Statement (DPS) Audit

(a) Perform compliance audit on the HKIRC DNSSEC operations and environment against the published DPS. This part is only required for the first- and third-year security audit services.

4.2.11 Internal Audit IT General Controls (Optional):

The following defines the scope of service to be provided by the Contractor. The Bidder can add or counter propose any tasks that they deem necessary for completeness and effectiveness

(a) User account access review and management.
(b) Change management processes.
(c) Backup and recovery procedures.
(d) Incident and problem management and response.
(e) Outsource management and procedure.
(f) Program development.
(g) Physical security and operation control.
(h) System configuration, database management, network perimeter management.
(i) Information Security.

4.2.12 IT Application Controls (Optional):

(a) Domain Name Registration System (DNRS), HR Systems (HRMS) or Finance Systems (M18) controls.
(b) Roles and permissions assigned within DNRS, HR Systems (HRMS) or Finance Systems (M18).
(c) Data integrity and security measures.

4.2.13 Operational Procedures (Optional):

(a) Review of system development life cycle (SDLC) practices.
(b) Evaluation of system architecture and resilience.
(c) Assessment of disaster recovery plans.

4.2.14 Documentation and Reporting (Optional):

(a) Prepare detailed findings and recommendations.

(b) Follow up on management action plans from previous audits.

(c) Provide regular updates to the Audit Committee.

4.3 DELIVERABLES

4.3.1 The Contractor shall develop and maintain a detailed project plan, provide regular project status updates, and deliver monthly progress reports to the HKIRC project team.

4.3.2 For each of the items listed in section 4.2 above, HKIRC expects detailed description of the findings as well as the resolutions, including the corrective, preventive, and detective measures applicable to HKIRC's actual environment, in the audit report.

4.3.3 Security audit report and the DNSSEC Practice Statement Audit report format and assessment severity classification:

(a) All reported findings should be characterized by either of the following:

Server / Device / IP address	This includes all physical and virtual servers 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 server).
User Applications	Any application that is not part of the installed system application and is created specifically for the company's business.

(b) 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.

4.3.4 DNSSEC Practice Statement Audit (item 4.2.10) requires a **separate audit report** on its own. Other requirements shall be combined in a single security audit report.

4.3.5 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 DNSSEC Practice Statement Audit (item 4.2.10).

4.3.6 The Contractor is required to present the audit scope to the Audit Committee each year to seek their comments as part of project planning. Presentation slides are required.

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

4.3.8 The Contractor shall also provide one briefing session to the Audit Committee. The session aims to explain the security audit findings and resolutions, and the follow-up review results of last year's security audit. Presentation slides are required.

4.3.9 Optionally, the Contractor might be requested to deliver a second briefing session to the Board for clarification or deep-diving into specific audit issues or area of interest, per request of senior management or board of directors.

4.4 MINIMIZING IMPACT TO PRODUCTION ENVIRONMENT

4.4.1 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.

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

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

4.4.4 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

4.5.1 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.

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

4.5.3 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.

4.5.4 In particular, for communications, the Contractor shall provide regular project status updates, and monthly progress reports to the HKIRC project team.

4.6 PROFESSIONAL STAFF REQUIREMENTS

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

4.6.2 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 detailed in the proposal. The team MUST be full-time staff directly employed by the Tenderer. **Subcontracting is forbidden** under this RFP. The requirements of the team are as follows:

(a) The project manager should:

(i) possess at least 10 years of working experience in IT security; and

(ii) have obtained ISO 27001 lead auditor or equivalent qualifications.

(iii) have obtained CISA, CISM, CISSP or equivalent qualifications.

(b) The team members should:

(i) possess at least 5 years of working experience in IT security; and

(ii) have obtained CISA, CISM, CISSP or equivalent qualifications.

(iii) have obtained CISP or equivalent qualifications.

(iv) have obtained technical assessment tester, such as CEH (Certified Ethical Hacker) or equivalent qualifications.

4.6.3 Replacement of project team members shall be agreed with HKIRC at the outset of the audit planning phase in each year. In the event of consultant changes during the year, consensus from HKIRC shall be sought as soon as practical. The replacement candidates shall possess comparable qualifications and working experience as the ones being replaced.

4.7 SERVICE LOCATION

4.7.1 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.

4.8 HKIRC STANDARDS, METHODOLOGIES AND QUALITY REQUIREMENTS

4.8.1 The Contractor shall comply with the following HKIRC regulations, policies, standards, guidelines, methodologies and quality requirements:

(a) Digital Policy Office, the Government:

(i) Baseline IT Security Policy

(ii) IT Security Guidelines

(iii) Practice Guide for Security Risk Assessment & Audit

(iv) Practice Guide for Penetration Testing

(v) Practice Guide for Information Security Incident Handling

(vi) Practice Guide for Website and Web Application Security

(vii) Practice Guide for Internet Gateway Security

(viii) Practice Guide for Cloud Computing Security

(ix) Practice Guide for Security Log Management

(x) The Interoperability Framework for the e-Government

(xi) Effective Systems Analysis and Design Guide

(xii) The Technology and System Architectures (GTSA) Framework

(xiii) Information Technology (IT) Security Policy

(b) ISO27001

(c) HK Cap. 486 Personal Data (Privacy) Ordinance

(d) No. 4 of 2025 Protection of Critical Infrastructures (Computer Systems) Ordinance

(e) China's Personal Information Protection Law (PIPL) (need to reference this regulation and do fair assessment)

(f) EU General Data Protection Regulation (GDPR) (need to reference this regulation and do fair assessment)

(g) Payment Card Industry Data Security Standard (PCI DSS)

The Contractor may refer to the HKIRC Procedures, Regulations, Guidelines and Standards for Contractors

4.8.2 Where necessary, the Contractor has to adopt adaptations to the methodologies and quality management system specified in Section 4.8 and those proposed in Technical Proposal. The Contractor shall seek agreement from HKIRC on any adaptations of the methodologies and quality management system that will be adopted for delivering the required services/products of this work assignment. For all agreed adaptations, the Contractor has to document the reason why such adaptations are adopted in relevant quality records.

5. INFORMATION SECURITY

5.1 The Tenderer shall be provided with a set of Non-Disclosure Agreement (NDA) after HKIRC received the company's Expression-of-Interest before the stipulated time.

5.2 By signing and returning the NDA, the Tenderer acknowledges and agrees that, if the Tenderer is selected as the Contractor, it shall be bounded by the HKIRC Information Security Policy.

5.3 The Contractor shall comply with the HKIRC Information Security Policy, to the extent that commensurate with its roles and responsibilities. The term "Contractor" hereby refers to staff members of the Contractor and its affiliates who are involved in this project.

5.4 A copy of the HKIRC Information Security Policy will be provided to the Tenderer upon its request after submission of a duly completed and signed NDA.

5.5 As proposals received by HKIRC are classified as "RESTRICTED", Tenderers are requested to mark "RESTRICTED" at the center-top of each page in black color. The proposal must be encrypted if transmitted electronically.

6. ANTI-COLLUSION

6.1 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.

6.2 Section 6.1 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.

6.3 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.

6.4 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

7.1 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.

7.2 Failure to so procure or any act of offering advantage referred to in section 7.1 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. COMPLIANCE WITH LAW

8.1 Notwithstanding anything to the contrary under the Agreement of this Project, HKIRC reserves the right to disqualify the Service Provider on the grounds that the Service Provider has engaged, is engaging, or is reasonably believed to have engaged or be engaging in acts or activities that are likely to cause or constitute the occurrence of offences endangering national security or otherwise the exclusion is necessary in the interest of national security, or is necessary to protect the public interest of Hong Kong, public morals, public order or public safety.

8.2 HKIRC may immediately terminate the Agreement of this Project upon the occurrence of any of the following events:
(a) the Service Provider has engaged or is engaging in acts or activities that are likely to constitute or cause the occurrence of offences endangering national security or which would otherwise be contrary to the interest of national security; or

(b) the continued engagement of the Service Provider or the continued performance of the Services is contrary to the interest of national security; or

(c) HKIRC reasonably believes that any of the events mentioned above is about to occur.

9. ETHICAL COMMITMENT

9.1 PREVENTION OF BRIBERY

9.1.1 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.

9.1.2 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.

9.2 DECLARATION OF INTEREST

9.2.1 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.

9.2.2 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.

9.2.3 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-sections 9.2.1 and 9.2.2.

9.3 HANDLING OF CONFIDENTIAL INFORMATION

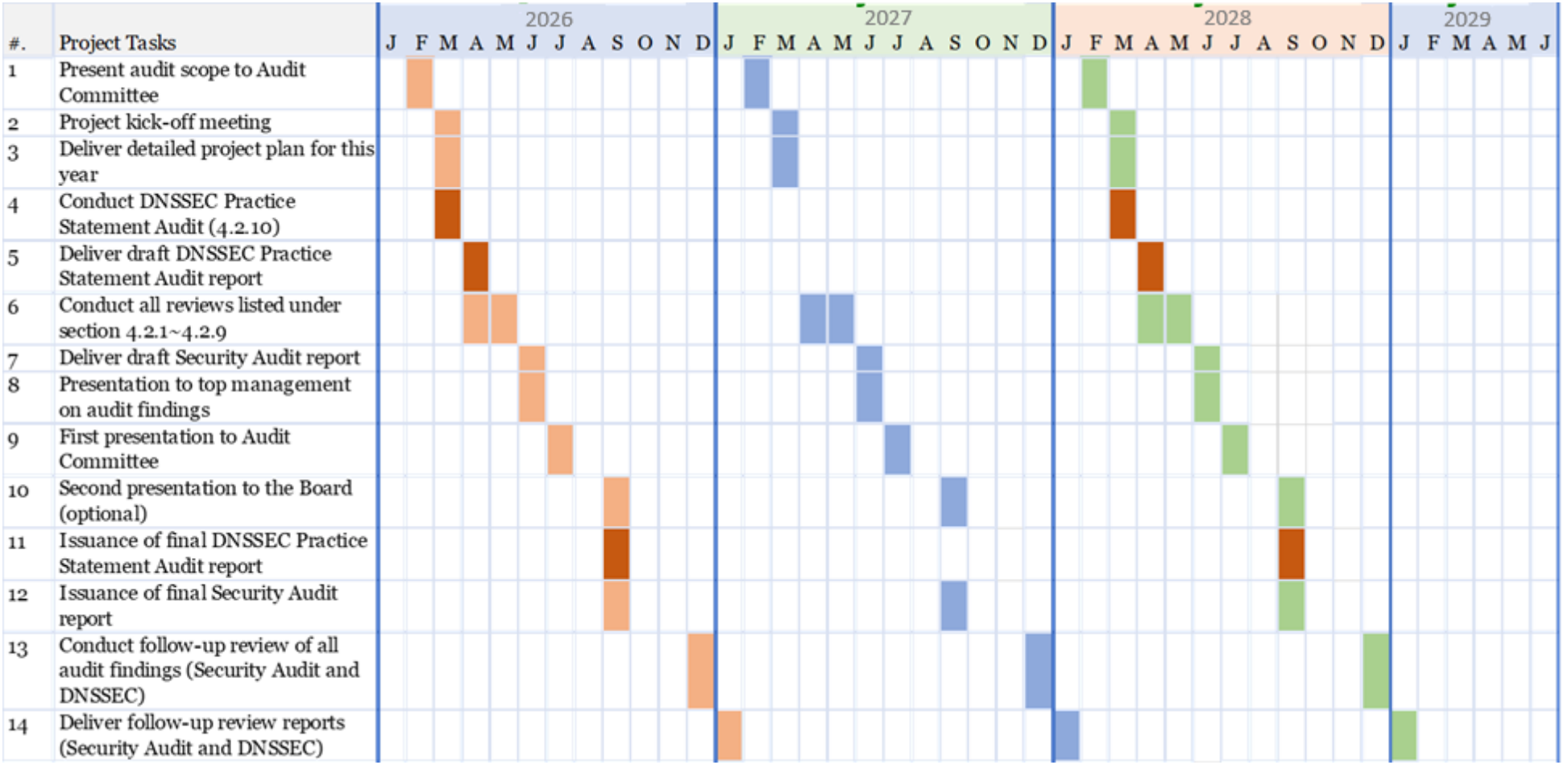
9.3.1 The Contractor shall not use or divulge, except for the purpose of this Contract, any information provided by the Organization in the Contract or in any subsequent correspondence or documentation, or any information obtained when conducting business under this Contract. Any disclosure to any person 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.

9.4 DECLARATION OF ETHICAL COMMITMENT

9.4.1 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-sections 9.1.1 to 9.3.1 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-sections 9.1.1 to 9.3.1 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.

10. PROJECT SCHEDULE

10.1 The tentative project schedule is proposed below. Contractors shall complete the fieldwork (including DNSSEC Practice Statement audit and Security Audit) within 3 months' time. The follow-up review is scheduled to commence around 6 months after deliver of the draft security audit report (step 9). The exact timing will be agreed with the Contractor in due course.



11. ENGAGEMENT OPTIONS & PAYMENT SCHEDULE

11.1 There may be minor change in the number of in-scope devices or applications in the second- and/or third-year audit. The resulting increase in professional fee shall be absorbed by the Contractor.

11.2 HKIRC reserve the right to exit the three-year contract anytime at its own discretion, with no penalty whatsoever, by giving the Contractor one-month advance notice.

11.3 The proposal shall be submitted on the basis of "fixed lump sum" for providing the required services outline under section 4.2.

11.4 Interested Tenderers shall provide the breakdown of (i) the cost, in Hong Kong Dollars, and (ii) man-day of all required services specified under section 4.2, on a year-by-year basis.

11.5 The Tenderers should make certain that prices quote is accurate before submitting their proposal.

11.6 Payment is made for the agreed services on a year-by-year basis. The following payment schedule is recommended but interested Tenderers may propose their own in the proposals. The payment schedule is the same for all three years.

	Milestone/Acceptance of Deliverables	**Payment %**
1.	Acceptance of project plan	10%
2.	Acceptance of final security audit report and the DNSSEC Practice Statement Audit report in the first and third year	70%
3.	Acceptance of final follow-up review report and the DNSSEC Practice Statement Follow-up Review report in the first and third year	20%
	TOTAL	**100%**

12. SERVICE ACCEPTANCE

12.1 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 fulfil 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.

13. SERVICE AGREEMENT NEGOTIATION AND SIGNATURE

13.1 The service agreement will be drawn up between the selected Contractor and HKIRC. HKIRC welcomes the Tenderer's proposal on a suitable service agreement for the project/service.

13.2 The service agreement must be signed by both parties within reasonable time 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.

14. ELEMENTS OF A STRONG PROPOSAL

14.1 All submitted proposal must follow 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 https://www.hkirc.hk	**Information Security Manager** YS LAM (Wilson) +852 23193849 ys.lam@hkirc.hk **Senior IT Manager** John LAM +852 2319 3811 john.lam@hkirc.hk
If you are not sure about the appropriate person to call, the receptionist can help you.	

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 Service 2026-2028:

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

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

(c) 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

(d) 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:

(a) reject the tender;

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

(c) 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)(a) 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) :

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

Name of Tenderer in English (in Block Letters) :

Date :

APPENDIX C – DECLARATION OF ETHICAL COMMITMENT

To: Hong Kong Internet Registration Corporation Limited (HKIRC)

Contract No.: _____

Title: Security Audit Service 2026-2028

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.

Authorized Signature & Company Chop :

_____

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

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

Name of Tenderer in English (in Block Letters) :

Date :

APPENDIX D – HKIRC PROPOSAL REQUIREMENTS

Proposal requirements	
Submission deadline	Please refer to section 1.7 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, two identical copies of the full proposal are required. The proposal shall be sent to the attention of YS LAM (Wilson) (Information Security Manager) or John LAM (Senior IT Manager).
Electronic copy	Electronic copy is mandatory. It shall be sent by email to ys.lam@hkirc.hk and john.lam@hkirc.hk .
Proposal format	Please refer to section D.2 below.
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) a persuasive section on the company background

(b) international recognize certification for security audit

(c) a strong and flexible service and tools meeting HKIRC requirements with minimum customization

(d) high level of interaction between HKIRC and the Contractor

(e) excellent fit with the capabilities and facilities of HKIRC

(f) strong company and project management team

D.1 PROPOSAL DEADLINE

All proposals must reach HKIRC as stated in section 1.7.

D.2 PROPOSAL CONTENT

The proposal should contain the following. Commonplace information expected under each major heading are elaborated on the next page.

1. Cover Page
2. Executive Summary
3. Conflict of Interest Declaration
4. Company Background
   - 4.1 Financial Situation
   - 4.2 Track Records
   - 4.3 Organization and management team
   - 4.4 Project team with credentials
   - 4.5 Company credentials
   - 4.6 Staff credentials
5. Methodology
6. Project management methodology
7. Understanding of our requirements
8. Knowledge and Advice on Projects/Services
9. Deliverable and Services level
10. Proposed Cost of Services and Payment Schedule
11. Implementation Timetable
12. Commercial and Payment Terms. e.g., Compensation for delay.

1. COVER PAGE

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

Cover Page		
Project Title		Security Audit Service 2026-2028
Project Manager	Name:	
	Title:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
Company	Contact person:	
	Title:	
	Company name:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
	Website:	

2. 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:

(a) Rationale for pursuing the project or service, the methodology/technology needed and the present state of the relevant methodology/technology.
(b) Brief description of the Tenderer's financial situation.

(c) Brief description of the Tenderer's facilities and experience on similar projects or services

3. CONFLICT OF INTEREST DECLARATION

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

4. 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.

5. METHODOLOGY

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

6. PROJECT MANAGEMENT METHODOLOGY

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

7. 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.

8. KNOWLEDGE AND ADVICE ON PROJECTS/SERVICES

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

9. 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**.

10. 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:

(a) Fixed setup cost
(b) 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.
(c) Equipment that is permanently placed or purchased for HKIRC to complete the project or service, if any.
(d) Subsequent support, maintenance, or consultation service.
(e) Other direct costs including services, materials, supplies, postage, traveling, pocket money, etc.

11. IMPLEMENTATION TIMETABLE

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

12. 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.

*** END ***