Consultation on the future arrangement of the SOA-QPS

The following are the comments from eWalker Consulting (HK) Ltd.

General comments

1. eWalker Consulting (HK) Ltd. participated in SOA services for Cat 4 since QPS2.
2. It was observed that the current services and awarded price (Cat 4 services) lowered to a rather unreasonable price. Low price is already damaging the overall market and the quality of the services. From our discussion with some participating vendors and B/Ds, they unofficially expressed that they already understand that due to the low awarded price, most of the reports are just a form of machine-generated reports. No analysis of the security risks and impacts could be found in the report.
3. Most projects' awarded prices would not be sufficient to support one equivalent consultant's monthly salary. As SOA-QPS actually affects the entire HK IT industry and market, HKSAR Government should try to create a much healthy IT market.
4. In QPS4 tender, there is a specific new score included – Innovation score. However, **innovation score may not be applicable to all 4 categories of services**. It is recommended that marking scheme should be adjusted to fit relevant services.
5. For the security requirement, it evolves based on the security posture of the industry and the adoption of new technology. Cause that may change faster than 3 years times. It is **advised that OGCIO may consider to re-establish a CyberSecurity Advisory board** to define the overall security requirement that aligns with government strategy. This will be able to enhance the overall security posture of the HKSAR government.
6. HKSAR Government should have a holistic security requirement that established and enforced the government, government organization and NGO. Currently, other organizations established and defined their requirement. Some may make reference to HKSAR Government policies and standards. As they are referring to the standards, it is advised that HKSAR Government should coordinate and jointly align the security requirement, standards in order to enhance the posture of the entire HKSAR Government.
7. It is recommended that HKSAR should consider establishing and providing guidance to HKSAR Primary and Secondary school an NGO. Currently, we have received the requirements from secondary schools and NGOs for requesting us to conduct security reviews for them. However, they usually do not have knowledge, standards or requirement for performing the review. Normally, they only used the OGCIO defined term "SRAA" but don't have the detailed requirements. In fact, more and more sensitive and data privacy leakage cases are from Primary and Secondary schools and NGOs. It is **recommended that HKSAR should consider working with EDB and SWD to develop, promote and enforce standardized security requirements to these organizations and sectors**.

PIA should be grouped to Cat 4

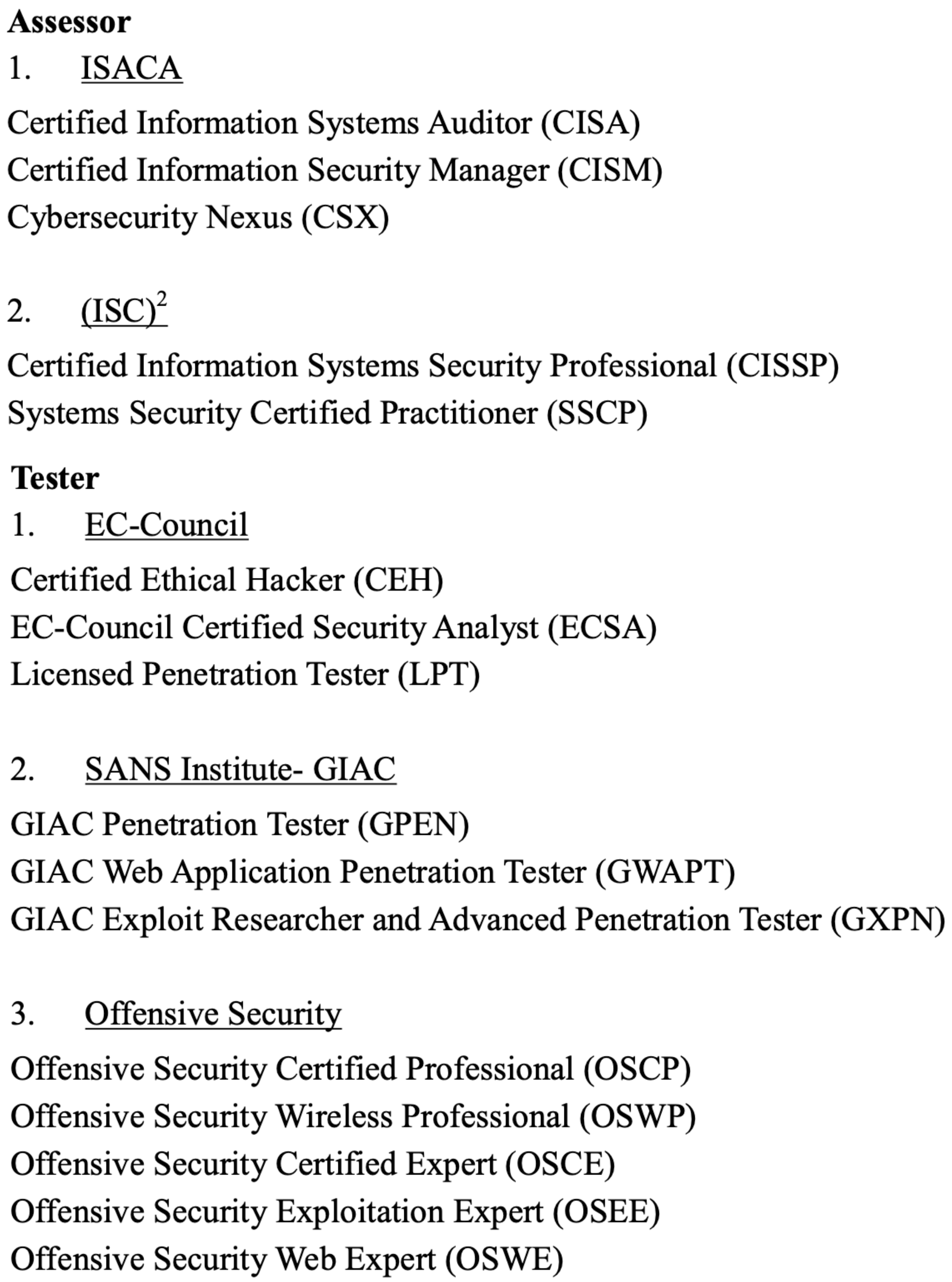
1. Regarding item 22 of the consultation paper, we agreed that Privacy Impact Assessment (PIA) should better be grouped to Cat 4.

2. We also **recommend that the Cat 4 services should be extended to overall Audit, Assessment and Assurance Services**. Security Risk Assessment, Audit Service is just part of the audit assessment and assurance services. Audit services could be extended to a specific kind of audit and assurance services such as ISO 27001 audit services. Privacy Impact Assessment could be considered as a specific kind of audit compliance services.
3. However, because Privacy Impact Assessment is not a pure technical review, it should NOT be using taking just purely CyberSecurity requirement. It should **also include the legal compliance requirement. The participating company should have legal and business compliance audit background.**
4. Besides, for PIA project requirement listed in the previous SOA-QPS4 has not been clearly defined. It should be clearly defined and **legal compliance requirements and business process analysis** should be defined clearly in the tender specification document.

SRAA, PIA, Penetration Test and Code Review specialist experience to Cat 4

1. In previous SOA-QPS staff qualification, it was usually defined using the universal template which defines the *Cat 5 specialist must of xxx certificate with n number of years*. However, that is **no longer applicable in this evolving market**.
2. Within the Cybersecurity market, **certifications are required for specialized service. E.g. there are certifications that specifically focus on penetration test service**, such as GIAC GPEN, CEH, OSCP, OSCE, etc. Similarly, CCSP and CCSK are specialized vendor neutral certifications for cloud security specialist and AWS Certified Security – Specialty certification for specialist that focus in AWS cloud environment.
3. Those with CISSP should be fit for those we specialized with a broad sense of CyberSecurity. These kinds of persons should be fit for IT security risk assessment but not reflecting they have knowledge in conducting penetration test. Also they may not have sufficient knowledge in Cloud Computing Security as well. **We recommended that for Cat 4 projects, more emphasis should be placed at the certificate and qualification instead.**
4. It is recommended that the **year of experience should be waived from the Cat n staff experience**. It does not mean that year of experience is no longer required, but on the contrary, this year of experience should be **referred back to the requirement of the certification requirement**. Many of the certifications have their own set of years of the experience requirement. For instance, CISSP already required 5+ years of cumulative paid work experience. This represents that CISSP could only be achieved by staff with working experience for IT knowledge in that industry. While for penetration test certifications such as GPEN and CEH, their certification is more focused on technical skills rather than just working experience. That is also aligned with the nature of CyberSecurity. It would be rather rare to have an experienced consultant to be focusing on both the technical security area and risk management area. Thus, it is recommended that OGCIO could adopt the scheme used by HKMA **to set up a Professional Development Programme (PDP) framework and working group to define the qualification for security professional**.
5. In fact, HKMA has developed a scheme for qualifying staff to perform iCast review. HKMA invited industry practitioners, representatives from banks to form a committee to define the Professional Development Programme (PDP) framework.

That PDP framework stated the requirement for different categories of the tester. The following are extracted lists from the HKMA PDP document.



Assessor

1. ISACA

Certified Information Systems Auditor (CISA)
Certified Information Security Manager (CISM)
Cybersecurity Nexus (CSX)

2. $(ISC)^2$

Certified Information Systems Security Professional (CISSP)
Systems Security Certified Practitioner (SSCP)

Tester

1. EC-Council

Certified Ethical Hacker (CEH)
EC-Council Certified Security Analyst (ECSA)
Licensed Penetration Tester (LPT)

2. SANS Institute- GIAC

GIAC Penetration Tester (GPEN)
GIAC Web Application Penetration Tester (GWAPT)
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

3. Offensive Security

Offensive Security Certified Professional (OSCP)
Offensive Security Wireless Professional (OSWP)
Offensive Security Certified Expert (OSCE)
Offensive Security Exploitation Expert (OSEE)
Offensive Security Web Expert (OSWE)

SRAA, PIA, Penetration Test, and Code Review requirement to Cat 4

1. Previously, in the ITPSA and QPS1, cybersecurity review should start from understanding and analyzing the threats of the environment exposed. When the application is newly developed and defined, threat analysis should be incorporated at the beginning of the design phase especially for the DevOps and Agile development methodology. However, in the recent SRAA review, we cannot identify the requirement of threat analysis included in the design document. Also, threat analysis review was not found in the SRAA review document. **Threat analysis should be incorporated into the requirement and be used as a source for SRAA review.**

2. For SRAA is considered as a good practice that adopted from ITPSA phase. However, the requirement, sections and review methodology should be revised according to the development methodology used. Previously, SRAA was developed based on waterfall model of development. With the use of Agile and DevOps development methodology and framework, the review should be starting from Security by Design. Though the word has been included in the S17, the entire thinking process and SRAA requirement has not incorporated the reviewed methodology. **It is recommended that the entire SRAA methodology should be defined to align with the requirement.**
3. While for the use of DevOps methodology, the organization that recommended DevOps methodology should have a project team that has DevOps knowledge as well as DevSecOps knowledge. With DevSecOps requirement incorporated, the organization should have security design included at the first phase and security consultant should be in place at the beginning to define the security requirement. That should be documented. Besides, the organization has to incorporated security tests in automatic review process for each release instead of just performing security review as in waterfall model. **The organization should ensure that they have security code scanning tools, SAST, DAST tools for performing code analysis and review as well as vulnerability scanning tools for performing vulnerability scanning at each update of code.**
4. Sample report requirement as well as process for different services should be outlined in order to ensure the quality of the services. Currently, the penetration test practice guide has incorporated the process but not the checklist or guidelines to be incorporated. While in SRAA practice guide, it has included the checklist but not the process list. It would be better that the requirement be standardized. Cloud computing-related test, guidelines have not been developed and standardized. **It is recommended that the requirement should be standardized and defined.**

<end of this document>