Consultation on the future arrangement of the SOA-QPS

The following are the comments from Cloud Security Alliance (HK & Macau Chapter)

General information

1. Cloud Security Alliance (HK & Macau Chapter), http://www.csahkm.org are the local chapter of the Cloud Security Alliance, http://www.cloudsecurityalliance.org
2. Our members and council members focus on CyberSecurity, Privacy aspects in Cloud Computing Environment and majority of our council members are from cloud service provider (CSP) and cloud security company.
3. Cloud Security Alliance (HK & Macau Chapter) council member also involved in conducting cloud security certification course (including CCSP of ISC2 and CCSK of CSA).

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. Cloud Security Alliance have developed a set of Privacy Level Agreement (PLA) and the GDPR Code of Conduct for GDPR privacy review, https://cloudsecurityalliance.org/privacy/gdpr/. **It is recommended that OGCIO can adopt the code of conduct and review checklist as part of the privacy impact assessment checklist**.

Security requirement for Cloud Computing Environment Project

1. In some previous implementation project, it was observed that security requirement were not explicitly stated in the project. Only existing security policies or requirements from other projects were adopted without any thorough analysis. In fact, in an implementation project, the Security Requirement should be defined and developed during design phase. Especially if a Cloud Computing Environment is to be adopted, data classification, security requirement, risk posture and associated threats should be determined before design phase of the project. Cause these requirements should be incorporated into the tender document before approaching the cloud service provider.
2. **Security Requirement should be incorporated** in the Cat 4 service tender document based on service model and deployment model of the cloud environment to be implemented. Cloud service model and deployment model adopted will be affecting the corresponding assessment that can be performed.
3. A core criteria in assessing the governance of cloud computing environment is the **Share Responsibility Model** of Cloud Computing Environment. Thus, a clear Roles and Responsibilities (R&R) matrix should be defined and confirmed in each cloud related project. **Besides, R&R review should be incorporated into the security requirement and review scope.**

DevOps changes

1. More projects were considered to be implemented using DevOps instead of waterfall model. However, in many implementation project tender, tenderer were given the opportunity to define the project management framework they choose.
2. If DevOps development framework is used, **it is recommended that Security Design Specification should be required from the beginning of the design** with the support and **implementation of automated security deployment tools**.
3. In DevOps development framework, CI/CD pipeline and Security test requirements should be included in the implementation cycle with proper software requirement. **The cost of DevOps tools should be implemented and covered in the implementation project.** In previous SRAA project, the security assessment tools are covered and handled by the SRAA service provider. However, in DevOps development framework, security review and assessment tools should be integrated to the CI/CD pipeline. The tools will be continuously used throughout the entire implementation period. If cost is included in SRAA project tender, due to the current tender bidding process, tenderer will choose to perform review without tools which will break the DevOps/DevSecOps and automated security review cycle.
4. Besides, the assessment tools become a continuous testing step but usually through automated process instead of manual human review process. Therefore, it is recommended that the security review and SRAA requirement has to be revised and **adjusted to continuous assessment review** instead of just finite/fixed rounds of SRAA assessment review.

Security by Design in Cloud Computing Environment

1. No matter the development framework is based on waterfall or DevOps framework, Cloud Security Standards should be incorporated into requirement from the **requirement collection and design phase**.
2. In order to ensure Security by Design in the implementation project, it is recommended that **Threat Modeling and Threat Analysis should be incorporated** at the design specification and requirement specification. In current security review projects, threat modelling and threat analysis are seldom incorporated into the SRAA projects. However, as more and more applications and systems were developed using new technology and innovative solutions, the developed systems may encounter threats different from traditional IT systems. With the use of cloud computing facilities, the attack surface may various depending on the nature and design of the application/system. Thus, it would be more appropriate to perform threat modelling and threat analysis based on the design of the system from the beginning. This method was used before at the first stage of security review in ITPSA review. However, after many rounds of review, this necessary and required steps were ignored by most security assessors.
3. Other than cloud computing architecture in SA&D review, **privacy, security configuration and policy, contract and SLA from CSP should be considered and collected for review** during the design and implementation phase of a project. Cloud computing is a mean of outsourcing, so SLA and contract are the important compliance and governance assessment tools. So SLA and contract review should be

considered as part of the important criteria to be considered within the SRAA review process.

4. If continuous development requirement are considered as part of the solution development and deployment requirement in cloud solution vendor, it is recommended **that B/D should include the development and deployment security requirement into the overall project scope within the SRAA project**.

Security Checklist and Report Format

1. Cloud Computing environment is quite different from traditional on-premises environment because of the change in Roles & Responsibilities within the selected service model and deployment model.
2. Also Cloud Computing environment is a special kind of outsourcing service. Thus, technological part of the project requirement may not be changed, but the access control, roles, and configuration review would become a critical assessment requirement. Thus, it is **recommended that Cloud Security Checklist should be defined and incorporated into the Security Assessment process**.
3. For Cloud Security review, it is necessary to review the security reports and posture of the CSP. It is a necessary component of the review process. Previously, in some OGCIO owned and managed infrastructure, review can only be performed on the environment owned and managed by the B/Ds. In Cloud Computing Environment, in order to achieve the Compliance Inheritance Requirement, all "Cloud Service Providers" have to ensure their security compliance report would be made available for "Cloud Service Customer" (that is, usually B/Ds and B/Ds appointed security assessor) to perform security review. **Thus, in SRAA, review of CSP reports should be considered as part of the review requirement.**
4. Cloud Control Matrix (CCM), https://cloudsecurityalliance.org/research/cloud-controls-matrix/, is the tools that widely used by CSP to review their security trust and compliance requirement. CCM is the core component for defining the security requirement for most cloud service provider according to the STAR audit program. CSA is enhancing and enriching the current version from v3 to v4 of the document. **It will become more auditor friendly tool which will be more applicable to be used for audit and assessment purpose for cloud solutions. It is also recommended that OGCIO should consider incorporating CCM as part of the standard audit review tools to be used.**
5. If the tenderer implements the solution using cloud computing facilities, no matter the solution will be implemented in GovCloud, public cloud or private cloud, **Security Assessment report should include cloud security checklists such as CCM**.

Security Professionals with specific knowledge

1. In implementation project, if project team is going to design and implement application in cloud computing environment, **at least one project team member** should **possess satisfactory level of cloud computing architecture** and **cloud computing security knowledge**. In previous project, it was observed that even SI that implemented Cloud Computing Environment do not have sufficient Cloud Computing Security knowledge.
2. Security Assessment of cloud computing environment and services implemented **should be performed by qualified cloud security professionals**. Security consultants

that participated in performing security review of cloud computing environment should reflect that they have possess relevant cloud security knowledge. They should have at least possess a vendor neutral certification cloud computing security certificate such as ISC2 CCSP, https://www.isc2.org/Certifications/CCSP, Cloud Security Alliance's CCSK, https://ccsk.cloudsecurityalliance.org/en or Cloud Security Alliance & ISACA's CCAK, https://cloudsecurityalliance.org/education/ccak/.

3. In some situation, B/D may also have to consider more specific certification such as AWS Certified Security – Specialty certification for specialist that focus in AWS cloud environment or AZ-500 for security requirement in Azure Cloud Computing environment.
4. Cause cloud computing environment should be rapid changing knowledge area, so it is recommended that Cloud Security Professionals should also continuous keep their attending latest and relevant training whenever possible. **Cloud Security Professionals should incorporate their CPE together with their certificate**s to reflect their knowledge and experience in particular knowledge area.

<end of this document>