

Doctor A Security's Comments on SOA-QPS2 Consultation Paper

Company Name: Doctor A Security Systems (HK) Limited

Service Category: 4

1. Regarding point 24 under (a) Categorisation of Services and Suppliers,
 - a. Continue NOT to divide the Service Category 4 into Major/Minor Group due to average amount awarded of most of the work assignment briefs was relatively small as compared to other Service Categories.
 - b. However, we suggest to divide the Service Category 4 based on service types since the services require distinct capabilities and experiences of the Contractors, e.g.
 - i. Group A – Security Risk Assessment and Security Audit; and Security Management Design & Implementation Services for Contractors that are good at consultancy and implementation;
 - ii. Group B – IT Security Monitoring and Incident Response Support Services for Contractors that are good at maintaining sophisticated, 7x24 infrastructure; and analyzing security events logs to identify security incidents.
 - c. Contractors could be in either one of the group or all group, depends on the capabilities and experiences of the Contractors.

2. Regarding point 33 under (d) Bidding Performance,
 - a. As of 5th April 2012 (around 32 months of the SOA-QPS2 Contract), there were over 250 SOA-QPS2 tenders in Service Category 4. In average, there were 7 to 8 tenders per month, which did require substantial efforts from the Contractors in the bidding process.
 - b. The current practice is that the Contractors must bid all tenders in the corresponding Service Category in order not to negatively affect the bidding performance rating.
 - c. However, in real situation the factors that influencing the intention for the Contractors to bid should include resources allocation, team competencies and other business related factors.
 - d. Also, it consumes substantial efforts for B/Ds to review the submitted proposals from all Contractors (i.e. 9) in the Service Category 4, especially for projects with awarded prices less than Hong Kong dollars fifty thousands, which could be simply handled by other procurement arrangement, such as Purchase Card. SOA-QPS2 was deemed by us too complicated for small amount service contracts.
 - e. Therefore we strongly recommend that i) B/Ds should be allowed to select a number (e.g. not less than fifty percent of the number of total Contractors) to receive the Work Assignment Briefs for preparing the proposals; ii) Contractors' bidding performance rating should not be affected if the participation rate reaches 70%. This will improve the

Doctor A Security's Comments on SOA-QPS2 Consultation Paper

efficiency for both Contractors and B/Ds in submitting and reviewing the tender submissions.

3. Regarding point 41 under (f) Sub-contracting,
 - a. Tenders of Security Services that requires highly sophisticated infrastructure for immediate responses (e.g. IT Security Monitoring and Incident Response Support Services) should not allow the use of sub-contractor to ensure the service quality and management.
4. Regarding point 44 under (g) Timing for Proposal Submission,
 - a. While there is a general requirement for the timeframe for proposal submissions, we also suggest that the timeframe of B/D for the notification of tender evaluation results should not exceed 1 month to allow the Contractors to have a more accurate bid projection and project planning.
5. Regarding point 47 under (h) Payment for Services,
 - a. Recommend B/D to issue tender not via SOA-QPS2 if the project scale is small and estimated price is less than fifty thousand Hong Kong dollars. SOA-QPS2 projects with prices less than fifty thousand Hong Kong dollars are not justified for the Contractors to comply the project management and administration requirements of the SOA-QPS2.
 - b. Allow B/D and Contractors to settle payment through p-card or other procurement arrangement and simplify project management and administration requirements for project awarded below fifty thousand Hong Kong dollars.
6. Regarding point 52 under (j) Project Delay,
 - a. The cause of project delay was not merely caused by the Contractors. Very often the project delays were due to:
 - i. delay in the readiness of the B/D system/ infrastructure for assessment/audit/monitoring;
 - ii. unreasonable delay of B/D in accepting the deliverables (e.g. arbitrary requests to Contractors in removing valid security findings, requests to Contractor to perform out-of-scope tasks, etc.)
 - b. Therefore measuring the Contractors' performance based on whether the projects complete on time without considering the overall situation and B/D involvements does not constitute a fair evaluation on the Contractors' performance.
 - c. We also strongly recommend the SOA-QPS2 administration to have guidelines to tackle unreasonable delay of B/D in accepting the deliverables (e.g. arbitrary requests to Contractors in removing valid security findings, requests to Contractor to perform out-of-scope tasks, etc.).

Doctor A Security's Comments on SOA-QPS2 Consultation Paper

7. Others – Evaluation of submitted proposals,
 - a. When evaluating submitted proposals, B/D should screen off the proposals with highest and lowest price to avoid some Contractors purposely use a very low price to bid the project that would adversely affect the project performance and quality.

8. Others – Work Assignment Brief Evaluation,
 - a. For Services that requires highly sophisticated infrastructure and specialized skillsets, such as IT Security Monitoring and Incident Response services, it is recommended that mandatory interviews should be arranged to review the capability of Contractors in delivering quality services, instead of simple document review based on pricing only. Evaluation from the interviews should have a significant role in selecting Contractors.

9. Others – Work Assignment Brief,
 - a. Suggest to rewrite the service specification of Security Risk Assessment and Security Monitoring in the Work Assignment Brief to reflect the latest industry best practices for the B/D and Contractors to follow.