MALTA RESOURCES AUTHORITY

MRA/135/2012

03rd September 2012

TENDER FOR ICT SECURITY RISK ASSESSMENT

With reference to services required sub-clause 8.4.1 (p. 26) and specifications sub-clause 8.5.1 (p. 27):

Question 1: Can you please clarify whether the scope of the information security risk assessment is limited to the business processes that are undertaken by the IT department?

The assessment is limited to the business processes undertaken by the IT department.

With reference to services required sub-clause 8.4.2 (p. 26) and specifications sub-clause 8.5.1 (p. 27):

Question 2: Can you give an approximate number and the type of infrastructure components (servers, network devices, etc.) that fall within the scope of the external penetration test?

Refer to reply to question 3.

Question 3: Can you give an approximate number and the type of infrastructure components (PCs, servers, network devices, etc.) that fall within the scope of the internal penetration test?

Network connected equipment: two modems, two routers, five switches, approximately 5 hubs, four servers, one cctv recorder, one pabx, approximately 10 printers/plotters, two scanners, approximately 60 pc's/laptops.

Question 4: Can you give an approximate number and the size/complexity of web applications that fall within the scope of the external penetration test?

Refer to reply to question 5.

Question 5: Can you give an approximate number and the size/complexity of web applications that fall within the scope of the internal penetration test?

IIS is installed on all servers. Most printers, pabx, routers plus cctv system are web-enabled.

Question 6: Can you briefly describe the purpose of in-scope web applications and state the kind of testing that is expected to be carried out against these systems (black-box/grey-box/white-box)?

Millennia Complex • 2nd Floor • Aldo Moro Road • Marsa • MRS 9065 • Malta
Tel: (+356) 22955000 • Fax: (+356) 22955200 • E-mail: enquiry@mra.org.mt

Black box testing

Question 7: Are you envisaging the possibility of the internal penetration test being carried out from a remote location or is it being expected that this exercise is carried out on-site?

On site.

With reference to specifications sub-clause 8.5.3 (pp. 27-28):

Question 8: Can you please state whether the Certified Information Systems Auditor (CISA) qualification is regarded as being equivalent to the listed professional certifications for the information security risk assessment?

Yes.

Question 9: If the CISA qualification is not regarded as being equivalent to the listed professional certifications for the information security risk assessment, can you provide a list of alternative qualifications (academic and/or professional) that are considered as being equivalent?

Not applicable.

Question 10: Can you provide a list of alternative qualifications (academic and/or professional) that are considered as being equivalent to the listed professional certifications for the penetration test?

Any alternatives, if provided for in the tender, will be considered on a case by case basis.