FEEDBACK FROM ORACLE CORPORATION
Date: 20 September 2008

PUBLIC CONSULTATION ON AO FRAMEWORK

Q1:
Agreed.

Q2:
Additional objectives to consider:

a) That AO maintains an independent and neutral (e.g. non-political) objective in the execution of its functions and provision of its services; as such, the AO shall not be unduly influenced or caused to perform its services that would contravene to such neutrality and objectivity

Q3:
Please ref. feedback to Q33.

Q4:
Although an accreditation scheme is a viable instrument in this case, one potential risk is the perceived "endorsement" that comes with accreditation, as well as the difficulty in growing / evolving the accreditation standards in tandem with AO market requirements and technology advancements.

Providing strict standards to the accreditation office and keeping them up-to-date may also pose a challenge.

Q5:
Clarifications needed for section 4.2 (a):

a) Are accreditations intended to be one-off exercises per AO?
b) If not, what frequency should AO's evaluate and satisfy their need accreditation?
c) Who ascertains if / when an AO needs to obtain a certain accreditation? Are AO's expected to self-regulate with respect to re/obtaining accreditations e.g. triggered by changes in business requirements and operating environment?
d) How are they sectors classified "critical sectors"?
e) Is accreditation of hardware and software that the AO employs also considered within the scope of this framework?

Clarifications needed for section 4.2 (b):

a) Do each sector regulator have a consistent and verifiable means of assessing if an online service is deemed critical?

Comment on Section 4.2 (b):
It makes sense in allowing sector regulators to make individual criticality assessments of online services so as to determine requirements to use accredited AOs.

However, we should take the opportunity at this developmental stage, to incorporate mechanisms that would circumvent the likely situations where AOs (who are serving multiple sectors) are faced with overlapping yet slightly different requirements – as is the common phenomenon faced by (and overwhelming) enterprises in highly regulated nations today.

Q6:
Agreed.

Comment to Section 5.2:

a) AOs should be also responsible and accountable for keeping up-to-date with pertinent technology.

Comment to Section 5.3:

b) Consider including the following considerations as major areas to be covered:
    a. IT Service Management
    b. IT Governance

Q7:
Agreed.
Such “safe harbour” provisions could indeed serve as a strong impetus for active AOs to seek accreditation.

Q8:
The liability exclusion provision as described may not be sufficient for potentially complex transactions. A more thoroughly spelt out exclusion schedule should be developed.

Q9:
Clarifications needed for Section 5.6:

a) Who in IDA shall be given the power to ascertain these contraventions; and what transparent, verifiable method will be used to ascertain them?

Comments to Section 5.6:

a) Given the severity of penalties, specifics details on each contravention should be more clearly and thoroughly spelt out

Q10:
Clarifications to Section 5.7 needed:

a) What are the limits to the proposed powers described herein?
b) Who in IDA can exercise such powers?

Q11:
Clarifications to Question 11 needed:

a) How will such powers be governed e.g. application of warrant through High Court?

Q12:
Clarification needed:

a) Quis custodiet ipsos custodes?

Q13:
Concur with what is proposed.
Further, specific controls applicable to each sector should also be considered.

Q14:
While ISO/IEC 27001 serves as a good framework and basis for organisations to achieve baseline level of security control across the operations wherein such framework is applied; it is by no means an infallible mechanism for preventing security compromises within the organisation concerned – especially to specialised areas of the AO's operation. This point must be stressed to any AO that is considering to attain ISO/IEC 27001 certification.

Agreed that AOs should use established standards specified.

Q15:
If the intention is to ensure an adequate and robust authentication infrastructure and operational environment within the AO; a more assured way is to require that the AO engages (from a panel of suitably qualified infocomm security risk management consultant vendors) a thorough and on-going program for security risk management services; so as to ensure that the security requirements are periodically refreshed to reflect the current state of threats within the organisation and outside.

Q16:
Periodic audits should also be enforced as part of the certification process.

Q17:
No comment.

Q18:
No comment.

Q19:
Yes.
Yes.

Q20:
Yes.
Pending the risk of complex technologies, concur to section 6.8.

Q21:
No comment.

Q22:
Concurred; AO’s should acknowledge any disclosure and liability.

Q23:
No comment.

Q24:
No comment.

Q25:
Agreed; and lifecycle objectives should be periodically audited.

Q26:
No comment.

Q27:
No comment.

Q28:
Should cater provisions for any unforeseeable abrupt and sudden discontinuation of services

Q29:
IDA should have the takeover rights if an AO decides to cease operations, which could affect end users' access to the systems.

Q30:
No comment.

Q31:
Agreed.

Q32:
No comment.

Q33:
End-note:
This paper sets out powerful and ambitious goals for a national authentication framework. The issue of chartering and regulating AOs is a critical one; otherwise it is very difficult to make progress on providing government and other services to all citizens. So definitely it is dealing with some of the key and significant issues in this area.

We are concerned about the degree of specificity of some of the technical requirements. How much input has been obtained from existing AOs in Singapore or elsewhere concerning these best practices? This is an area in which some experimental trials and inputs from other countries and experiences would be very valuable. We are concerned that too much detail is being specified at this early stage.

We would strongly encourage IDA to reach out to communities and countries that are also moving in this direction. Specifically, the Liberty Alliance e-Govt Special Interest Group has a number of active participants and documents available.

More information is available from:
http://wiki.projectliberty.org/index.php/EGovSIG

We would be most keen in exploring with IDA the development of such an experimental trial; as well as assist IDA in facilitating the communications with the Liberty Alliance e-Govt SIG and other such entities.

Compiled by:

Wong Loke Yeow
Director, Business Development
Oracle Corporation
Tel: +65 8112 6783
Fax: +65 6436 1626