CCC EXHIBIT

4. *What do you think could be done to ensure compliance with information security requirements?*

Departmental response

In relation to cyber security, one of the key focus of the Cyber Security Group is to promote and support a strong cyber security culture within Queensland Health through the cyber security awareness program. The awareness program is designed to help staff to realise, recognise and respond to cyber security concerns.

In relation to information privacy, a review of the *Information Privacy Act 2009* with one set of Privacy Principles for all agencies and updates to take into account the advancement of technology and its use in agencies. Implementing a compliance requirement with a mandatory reporting and sanction aspect, similar to that which is required by the *Privacy Act 1988* (Cth).

Focussing on the way privacy is approached by adopting a more positive 'Privacy by Design' approach, particularly in the establishment phase of new systems/projects/programs.

QAS response

Enhanced information security compliance can be achieved with the progressive implementation of the QAS ISMS in terms of its respective dimensions.

Information security considerations must be implemented seamlessly in all relevant QAS operational business processes and service delivery activities, such that it becomes common place and second nature.

An officer-centric approach should be adopted with information security integrated into the responsibilities of the respective organisational roles. 'People' are the weakest link in any information security model, so must be educated, aware, questioning and proactive, as it relates to information security.

This will require organisational change with a strong focus on business process engineering, strengthening information security awareness, communications, promulgation, upskilling and compliance assessment. Information security must be embedded as a fundamental aspect of the organisation, with the benefits articulated.

The building of an information security culture requires an end-to-end approach which can be progressively integrated and reinforced in terms of:

- ICT Acceptable use and user responsibilities
- Access management
- Mobile devices
- Asset management
- Human resources
- Physical security
- Supplier management
- Incident management; and
- Business continuity management.

With the rapid evolution of technology and digital disruption, coupled with social engineering becoming so sophisticated, organisation's must constantly strive to enhance, strengthen and mature their organisation's information security capabilities