Appendix 7

Prudential – Investment, Insurance Intermediation and Banking Rules (PRU)

*In this attachment underlining indicates new text and striking through indicates deleted text.

...

6.6 Information Technology (IT) systems

6.6.1 An Authorised Person must establish and maintain:

(a) appropriate information technology policies and processes to identify, assess, monitor and manage technology risks; and

(b) appropriate and sound information technology infrastructure to meet its current and projected business requirements, under normal circumstances and in periods of stress, which ensures data and system integrity, security and availability and supports integrated and comprehensive risk management.

Guidance

1. IT systems include the computer systems and information technology infrastructure required for the automation of processes and systems, such as application software, operating system software, network infrastructure, and desktop, server and mainframe hardware.

2. An Authorised Person should consider the following in establishing its systems and controls for the management of IT system risks:

   a. governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the Authorised Person's business objectives;

   b. an Authorised Person's organisation and reporting structure for technology operations, including adequacy of senior management oversight; and

   c. the appropriateness of the systems acquisition, development and maintenance activities, including the allocation of responsibilities between IT development and operational areas.

3. GEN 3.5 contains additional requirements that apply to Authorised Persons in relation to Cyber Risk management.

6.7 Information security

6.7.1 An Authorised Person must establish and maintain appropriate systems and controls to manage its information security risk.

Guidance

1. In establishing its systems and controls to address information security risks, an Authorised Person should have regard to:

   a. confidentiality: information should be accessible only to Persons or systems with appropriate authority, which may require firewalls within a system, as well as entry restrictions;

   b. the risk of loss or theft of customer data;

   c. integrity: safeguarding the accuracy and completeness of information and its processing;

   d. non-repudiation and accountability: ensuring that the Person or system that processed the information cannot deny their actions; and

   e. internal security: including premises security, staff vetting; access rights and portable media, staff internet and email access, encryption, safe disposal of customer data, and training and awareness.

2. GEN 3.5 contains additional requirements that apply to Authorised Persons in relation to Cyber Risk management.

...