Chapter 13

Operational risk: systems and controls for insurers

13.7 Processes and systems

13.7.1 G A *firm* should establish and maintain appropriate systems and controls for managing operational risks that can arise from inadequacies or failures in its processes and systems (and, as appropriate, the systems and processes of third party suppliers, agents and others). In doing so a *firm* should have regard to:

(1) the importance and complexity of processes and systems used in the end-to-end operating cycle for products and activities (for example, the level of integration of systems);

(2) controls that will help it to prevent system and process failures or identify them to permit prompt rectification (including pre-approval or reconciliation processes);

(3) whether the design and use of its processes and systems allow it to comply adequately with regulatory and other requirements;

(4) its arrangements for the continuity of operations in the event that a significant process or system becomes unavailable or is destroyed; and

(5) the importance of monitoring indicators of process or system risk (including reconciliation exceptions, compensation payments for *client* losses and documentation errors) and experience of operational losses and exposures.

13

Internal documentation

13.7.2 G Internal documentation may enhance understanding and aid continuity of operations, so a *firm* should ensure the adequacy of its internal documentation of processes and systems (including how documentation is developed, maintained and distributed) in managing operational risk.

External documentation

13.7.3 G A *firm* may use external documentation (including contracts, transaction statements or advertising brochures) to define or clarify terms and conditions for its products or activities, its business strategy (for example, including through press statements), or its brand. Inappropriate or inaccurate information in external documents can lead to significant operational exposure.

13.7.4 G A *firm* should ensure the adequacy of its processes and systems to review external documentation prior to issue (including review by its compliance,

legal and marketing departments or by appropriately qualified external advisers). In doing so, a *firm* should have regard to:

(1) compliance with applicable regulatory and other requirements;

(2) the extent to which its documentation uses standard terms (that are widely recognised, and have been tested in the courts) or non-standard terms (whose meaning may not yet be settled or whose effectiveness may be uncertain);

(3) the manner in which its documentation is issued; and

(4) the extent to which confirmation of acceptance is required (including by *customer* signature or counterparty confirmation).

IT systems

13.7.5 G IT systems include the computer systems and infrastructure required for the automation of processes, such as application and operating system software; network infrastructure; and desktop, server, and mainframe hardware. Automation may reduce a *firm's* exposure to some 'people risks' (including by reducing human errors or controlling access rights to enable segregation of duties), but will increase its dependency on the reliability of its IT systems.

13.7.6 G A *firm* should establish and maintain appropriate systems and controls for the management of its IT system risks, having regard to:

(1) its organisation and reporting structure for technology operations (including the adequacy of senior management oversight);

(2) the extent to which technology requirements are addressed in its business strategy;

(3) the appropriateness of its systems acquisition, development and maintenance activities (including the allocation of responsibilities between IT development and operational areas, processes for embedding security requirements into systems); and

(4) the appropriateness of its activities supporting the operation of IT systems (including the allocation of responsibilities between business and technology areas).

Information security

13.7.7 G Failures in processing information (whether physical, electronic or known by *employees* but not recorded) or of the security of the systems that maintain it can lead to significant operational losses. A *firm* should establish and maintain appropriate systems and controls to manage its information security risks. In doing so, a *firm* should have regard to:

(1) 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;

(2) integrity: safeguarding the accuracy and completeness of information and its processing;

(3) availability and authentication: ensuring that appropriately authorised *persons* or systems have access to the information when required and that their identity is verified;

(4) non-repudiation and accountability: ensuring that the *person* or system that processed the information cannot deny their actions.

13.7.8 G A *firm* should ensure the adequacy of the systems and controls used to protect the processing and security of its information, and should have regard to established security standards such as ISO17799 (Information Security Management).

Geographic location

13.7.9 G Operating processes and systems at separate geographic locations may alter a *firm*'s operational risk profile (including by allowing alternative sites for the continuity of operations). A *firm* should understand the effect of any differences in processes and systems at each of its locations, particularly if they are in different countries, having regard to:

(1) the business operating environment of each country (for example, the likelihood and impact of political disruptions or cultural differences on the provision of services);

(2) relevant local regulatory and other requirements regarding data protection and transfer;

(3) the extent to which local regulatory and other requirements may restrict its ability to meet regulatory obligations in the *United Kingdom* (for example, access to information by the *FCA* and local restrictions on internal or external audit); and

(4) the timeliness of information flows to and from its headquarters and whether the level of delegated authority and the risk management structures of the overseas operation are compatible with the *firm*'s head office arrangements.