Chapter 13

Operational risk: systems and controls for insurers

13.8 External events and other changes

13.8.1 G The exposure of a *firm* to operational risk may increase during times of significant change to its organisation, infrastructure and business operating environment (for example, following a corporate restructure or changes in regulatory requirements). Before, during, and after expected changes, a *firm* should assess and monitor their effect on its risk profile, including with regard to:

(1) untrained or de-motivated *employees* or a significant loss of *employees* during the period of change, or subsequently;

(2) inadequate human resources or inexperienced *employees* carrying out routine business activities owing to the prioritisation of resources to the programme or project;

(3) process or system instability and poor management information due to failures in integration or increased demand; and

(4) inadequate or inappropriate processes following business re-engineering.

13.8.2 G A *firm* should establish and maintain appropriate systems and controls for the management of the risks involved in expected changes, such as by ensuring:

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

(2) the adequacy of the management processes and systems for managing the change (including planning, approval, implementation and review processes); and

(3) the adequacy of its strategy for communicating changes in systems and controls to its *employees*.

Unexpected changes and business continuity management

13.8.3 G SYSC 3.2.19 G provides high level *guidance* on business continuity. This section provides additional *guidance* on managing business continuity in the context of operational risk.

13.8.4 G The high level requirement for appropriate systems and controls at ■ SYSC 3.1.1 R applies at all times, including when a business continuity plan is invoked. However, the *FCA* recognises that, in an emergency, a *firm* may be unable to comply with a particular *rule* and the conditions for relief are outlined in ■ GEN 1.3 (Emergency).

13.8.5 G A *firm* should consider the likelihood and impact of a disruption to the continuity of its operations from unexpected events. This should include assessing the disruptions to which it is particularly susceptible (and the likely timescale of those disruptions) including through:

(1) loss or failure of internal and external resources (such as people, systems and other assets);

(2) the loss or corruption of its information; and

(3) external events (such as vandalism, war and "acts of God").

13.8.6 G A *firm* should implement appropriate arrangements to maintain the continuity of its operations. A *firm* should act to reduce both the likelihood of a disruption (including by succession planning, systems resilience and dual processing); and the impact of a disruption (including by contingency arrangements and insurance).

13.8.7 G A *firm* should document its strategy for maintaining continuity of its operations, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy. A *firm* should establish:

(1) formal business continuity plans that outline arrangements to reduce the impact of a short, medium or long-term disruption, including:

(a) resource requirements such as people, systems and other assets, and arrangements for obtaining these resources;

(b) the recovery priorities for the *firm's* operations; and

(c) communication arrangements for internal and external concerned parties (including the *FCA*, *clients* and the press);

(2) escalation and invocation plans that outline the processes for implementing the business continuity plans, together with relevant contact information;

(3) processes to validate the integrity of information affected by the disruption; and

(4) processes to review and update (1) to (3) following changes to the *firm's* operations or risk profile (including changes identified through testing).

13.8.8 G The use of an alternative site for recovery of operations is common practice in business continuity management. A *firm* that uses an alternative site

should assess the appropriateness of the site, particularly for location, speed of recovery and adequacy of resources. Where a site is shared, a *firm* should evaluate the risk of multiple calls on shared resources and adjust its plans accordingly.