
Title: Why directors of FSA regulated firms cannot ignore Business Continuity

Whilst the Financial Services industry has been required by their Regulator(s) for many years to have appropriate Business Continuity arrangements in place it is only recently that the FSA has begun to define what 'appropriate' means.

In late 2002, the FSA commissioned a review of the Business Continuity practices of 12 major UK Financial Groups. From this review, certain observed practices were categorised as Standard Practice and Good practice. This categorisation has become a basis for other FSA initiatives and recent rule changes. Sixteen specific regulatory risks pertaining to the adequacy of Business Continuity were identified.

In 2005 they are undertaking another benchmarking exercise but with a much larger sample, probably of the order of 100. Once again, the findings will drive their requirements and expectations on member firms by further defining, and inevitably raising, acceptable standards of practice.

The FSA themselves, along with the Treasury and Bank of England, have been significantly developing, communicating and exercising their own arrangements for dealing with major financial system interruptions. This allows them to review other's arrangements from a position of strength and experience.

The FSA, through its Risk Based supervision policy, has also published a risk assessment framework for Business Continuity control risks. This further defines their thinking on appropriate Business Continuity arrangements and will determine their monitoring approach.

The recent introduction of General Insurance and Mortgage companies into the FSA regulated arena, required those companies applying for authorisation to answer significant questions regarding their IT infrastructure, its maintenance and resilience and, when all else fails, what Business Continuity arrangements were in place. They asked whether the arrangements extended beyond IT.

Following consultation, various elements of the Senior management arrangements, Systems and Controls regulatory document have been expanded, particularly the Business Continuity Section which has expanded from one paragraph to seven. It is important to recognise that 'Consultation' and subsequent published rules are the method of communicating what firms need to do to satisfy the regulator and is considered 'fair warning' that the appropriate areas of the firm should have accepted any new obligations by the time the rules are published; there is no 'grace period'.

A summary of these developing obligations and expectations could be –

- Business Continuity management systems must address many levels of risk specifically including financial, regulatory, legal and reputational.
- Managing such risks is considered the responsibility of senior, if not authorised, management of the company; ownership of Business Continuity is expected to be at Board Level and not limited to one Director. Ownership and visible control is evidenced by board level discussion and minuted conclusions.
- Arrangements must be tested and proven on a regular basis. The tests must exercise and prove responses to all significant risks, many of which are only peripherally linked to IT. Systems Recovery is not Business Recovery. Lessons learnt from exercises MUST be actioned.
- Arrangements must be appropriate to the risks identified by senior management. Exercising is one critical measure of the adequacy of the arrangements if the scope is sufficiently broad – material, facilities, sites, systems, people, and organisation. Conclusions on the results of each exercise should be drawn by senior management, following input from their subordinates/representatives.
- Given the requirement for senior management ownership, specification and oversight of these Business Continuity arrangements, inspection visits are more likely to address senior management knowledge and understanding rather than operational preparation.
- Invoking a firm's Business Continuity plan is now a specific event requiring immediate notification to the FSA. Scrutiny of the firm's response to any major interruption will be more immediate and more intense.