

Systems Based Auditing Control Matrices: Series 6

INTRODUCTION

Risk management is probably the most-talked about audit subject today; indeed, there are some who have based their audit methodology on risk in the form of risk-based internal auditing (RBIA).

However, whilst acknowledging the importance of risk is commendable, it is disappointing that there is often little if any mention of business continuity, which is far more important.

Although risk management can reduce the likelihood (and thereby the impact) of some hazards/ events occurring, it is not infallible and does not guarantee success. A prime recent example is the Buncefield oil storage depot explosion and fire that occurred in the early hours of 11 December 2005. The immediate impact was obviously felt by the depot, but what about the after-effects of this and other such disasters:

- how many businesses suffered severe physical and economic damage as a result of something their own risk management systems could not prevent?
- how many of these businesses have ceased trading, or have still not fully recovered their previous trading positions, as a result of disasters?

Business continuity goes beyond the scope of risk management and works on the premise that some hazards/events will occur. It seeks, therefore, to identify and implement the actions necessary to enable the business to recover and resume trading, thereby ensuring its survival.

CIPFA's Systems Based Auditing Control Matrices: Series 5 contained risk management papers that were based on the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management – Integrated Framework. Series 6 builds on the close link to risk management in that it contains three matrices covering business continuity in the form of:

- Business Continuity Management
- Information Technology Service Contingency Management
- Civil Emergencies – Local Authorities.

And, indeed, the fourth matrix, covering the important area of performance indicators and data quality, carries on the theme of business continuity as it covers ensuring that data is recoverable and available should an event happen.

The Series 6 matrices are again written by Exeter City Council's Internal Audit team, winners in 2007 of the prestigious Sir Harry Page Merit Award for technical innovation for producing the five non-financial matrices making up Series 5.

Each matrix consists of three documents:

Hazard Identification Document – identifies hazards/events that may adversely affect the system. Importantly, the HID also shows what the possible consequences are, without which it may be difficult to identify and 'value' the impacts. Finally, it shows the expected mitigating controls and countermeasures.

Internal Control Questionnaire – the purpose of which is to ascertain if the expected mitigation is in place or not. Importantly, as part of Exeter's risk-based SBA approach, the questions purposely do not ask about the quality and effectiveness of the controls and countermeasures.

Compliance Tests Papers – these tests are devised to check whether the controls and countermeasures that management have established are actually in place and working.

In addition, they are also designed to assess the quality and effectiveness of the controls and countermeasures by, for example:

- assessing the effectiveness of communication by checking directly with employees their awareness of policies, procedures, etc
- examining policy documents and the like to assess whether they are clear and concise.

Ed Heaton

Head of Audit Exeter City Council