SYSTEM BASED AUDITING

Control Matrices
IT Governance Series 8

1. INTRODUCTION

1 IT governance (ITG), which is part of corporate governance, requires that IT performance and the associated risks are effectively managed, and that those responsible for making decisions are accountable for their actions and able to justify their investment in IT. Therefore greater accountability is needed to ensure that the investments made are in the best interest of the organisation and its stakeholders.

2 This requirement represents a big change, for traditionally many organisations simply appointed IT professionals to manage their IT services, and then made huge financial investments on their say-so without seeking assurance that these would achieve real worth and measurable outcomes. To enable IT performance to be measured, a number of standards, frameworks and measures have been developed, such as:

- COBIT – Control Objectives for Information and Related Technology
- ISO27001 – *Code of Practice for Information Security Management*
- ISO38500 – *Corporate Governance of Information Technology*
- ITIL – IT Infrastructure Library.

3 These and other sources were referred to in order to devise these ITG Systems Based Auditing control matrices.

2. SYSTEMS BASED AUDITING

4 There is currently misunderstanding and confusion about what Systems Based Auditing (SBA) is, resulting in such statements as '*Risk Based Internal Auditing (RBIA) supersedes SBA*', yet in fact RBIA uses SBA. The root cause of this problem is the misuse of the word 'Based' which has resulted in Systems Auditing (eg financial systems) now being referred to as Systems *Based* Auditing, when it is not.

5 SBA was devised in the 1960s/1970s to replace the auditing method that was then in use, which solely tested the output of systems (eg matching cheques to creditors' invoices). SBA concentrated on examining the effectiveness of systems by, for example, checking that adequate control measures were in operation, such as that batch control totals were used for inputting data. SBA therefore replaced auditing based upon the outputs of systems, to *Auditing Based* upon the way *Systems* operate and their effectiveness, hence why it is called *Systems Based Auditing*.

3. USING THE SERIES 8 CONTROL MATRICES

6 The purpose of these matrices is to provide tests for use by general and specialist IT auditors, as well as those concerned with IT governance. They are non-sector-specific and so can be used in the public, the private and the third sector. By undertaking these tests, a succinct overview will be obtained of the extent that IT governance standards, etc are being met, and in turn this will enable a gap analysis to be undertaken so that areas for improvement can be clearly identified and reported to senior management and the managing body.

7 Series 8 consists of a Hazard Identification Document (the purpose of which is self-evident) and 18 control matrices. The first control matrix (ITG01 General) covers the overall 'top-level' direction and management, and includes the strategic plan, information architecture and technological direction. It is therefore suggested that the ITG01 compliance and assurance tests are undertaken before any of the other 17 matrices. However, this is not essential – if a particular area gives concern or is considered high risk, then the tests contained in the relevant matrix can be undertaken before ITG01.

8 A notable difference in this series is that the Internal Control Questionnaires have been dispensed with (as they were considered superfluous), and that as well as Compliance Test Papers (CTPs), there are also now Assurance Test Papers (ATPs). The latter were introduced by the authors, Exeter City Council's Internal Auditors, as part of the Enhanced Systems Based Auditing (ESBA) and Enterprise Risk Management Auditing (ERMA) approach they devised to further incorporate best practice risk management techniques, particularly those of COSO.

9 COSO is the abbreviation of the Committee of Sponsoring Organizations of the Treadway Commission, of which the Institute of Internal Auditors is one of the five sponsors. In September 2004 COSO published the *Enterprise Risk Management – Integrated Framework*. One of its key messages is that it is essential for good corporate governance and effective enterprise risk management that when organisations, for example:

- establish policies, standards, rules and procedures
- allocate roles and responsibilities,

that they actually tell the target audience about them, provide them with training where appropriate, and regularly remind them. The ATPs therefore serve as a means of assessing how well, or otherwise, the organisation has (for example) made its employees aware of what they are and what they are not allowed to do, and thereby identify weaknesses that can be addressed, thus avoiding potential management problems.

10 It is suggested that, once the various IT governance control matrices have been tested, for future audits only selective testing is undertaken rather than all of the CTPs and ATPs. Selective testing should only be undertaken for high risk areas (based upon risk assessments) or vulnerabilities, and for those areas where the results of previous testing were far from satisfactory. It should also be borne in mind that if the result of the ATP testing was satisfactory, and there have been no new staff appointments, that there is no need to retest.

Edmund Heaton
Head of Audit
Exeter City Council