

Systems Based Auditing Control Matrices: Series 1 & 2 2006 (Fully Revised Edition)

INTRODUCTION

Systems based auditing (SBA) is the most efficient auditing methodology to provide assurances that the systems of internal control established by management are operating properly. In recent years, attention has focused on the need for an effective system of internal control, particularly in response to well-publicised financial scandals and control failures.

Increasingly, managers and auditors are being required to provide statements to boards, councils and committees, and often publicly, that the system of internal control put in place by management is adequate and effective. Local government, for example, is now required to produce an annual Statement on Internal Control. SBA is a valuable tool to support the assurances to be given about the adequacy of internal controls within the organisation.

Systems based auditing is not new; the methodology has been around for many years, but some organisations have not yet implemented it properly and misunderstand what SBA actually is. SBA is a methodology for identifying weaknesses/risks in systems and the controls management have established to address the weaknesses/risks, and for testing the controls to check they are working effectively in order to provide assurance to management.

The role of audit is changing and auditors need to adopt a risk based approach to their work that integrates with the organisation's risk management strategy. Auditors need to assess the adequacy of their organisation's risk management systems, and ensure that best use is made of audit's resources. Adoption of a risk based approach requires that the risks identified and the actions proposed/taken by management to minimise these be assessed for effectiveness.

The risk based approach should be extended to include auditing of the main/fundamental financial systems (eg creditors, payroll, debtors, etc). As part of Exeter City Council's risk based SBA approach, the Internal Control Questionnaires and Compliance Tests have been broken down into sub-headings to enable easy identification of areas of weakness/risk so that managers can address potential problems. This approach ensures that audit resources are used to best effect and allows only minimal assurance testing to be undertaken on areas where it is considered that there are adequate levels of internal control.

Whilst managers have a duty to review and test their own controls, it is important that independent auditors also review and test controls. SBA provides a methodology for review by managers and auditors alike.

Both internal and external auditors are concerned with internal controls and need to review and test them in order to gain assurance. However, there are significant differences between the roles of the two sets of auditors. There is a need for a co-

ordinated approach between the two to ensure that all areas of auditing responsibility are covered. A systems based auditing methodology which is aimed at achieving this co-ordinated approach should meet the objectives of both internal and external auditors, and help them to reduce the total amount of audit effort. This is much easier to achieve where both sets of auditors use the same methodology. Such an approach enables:

- a co-ordinated and efficient audit with no duplication of effort
- external auditors to place maximum reliance on internal audit's work
- audit effort to be focused more effectively.

This last point is vital because all audited bodies, particularly those delivering public services, are under increasing pressure to maximise their use of resources and to minimise costs. The aim should be an agreement between internal and external auditors each year on the key areas to be reviewed and tested and on an appropriate division of duties, in order to achieve best value.

It is with this aim that these control matrices have been developed for both internal and external auditors. CIPFA's *A Guide to Systems Based Auditing* draws on the approach, standards and guidance of a variety of audit and regulatory bodies, including the Audit Commission.

The approach used

Within each system, there are three elements to the control matrices:

- Hazard Identification Document (HID)
- Internal Control Questionnaire (ICQ)
- Compliance Tests Papers (CTP).

These documents have been developed by Exeter City Council's Internal Audit Unit as part of its 'risk based' SBA approach.

Hazard Identification Document

The HID has replaced the Risk Identifier Document (used in the original series) in order to emphasise, and make the approach more in line with, risk management. The HID provides a structured approach for:

- documenting likely hazards affecting systems
- identifying possible consequences
- determining controls and countermeasures that are expected to be in place in order to minimise risks.
- Hazards are anything that has potential to cause harm. Harm includes:
 - personal injury or ill health
 - loss or damage to assets and property
 - loss of reputation
 - financial loss
 - environmental pollution.

To identify potential risks, hazards are risk assessed to ascertain the *impacts/consequences* and the *likelihood* of them happening.

Each system's hazards are considered under the following headings:

- authority – is the system covered by standing orders/financial regulations, statutes and regulations, professional guidance?
- occurrence – are transactions real and not fictitious and is there documentation or proof to support them?
- completeness – were all transactions recorded and all relevant records and accounts updated?
- measurement – were transactions correctly calculated and valued?
- timeliness – were transactions initiated and recorded promptly?
- regularity – as defined in its widest sense, to mean were the transactions legitimate and appropriate (thereby incorporating propriety)?

Each expected control and countermeasure on the HID is cross-referenced to the relevant part of the ICQ.

Internal Control Questionnaire

The ICQ is cross-referenced to the 'Expected controls and countermeasures' column in the HID and broken down into the various sub-systems or procedures in order to enhance risk assessment.

The ICQ provides a means of establishing whether the expected controls and countermeasures are in place. The questions are designed so that a 'yes' answer indicates that the expected control is in place, and a 'no' answer that it is not. The auditor should in any case supplement ICQs with systems documentation, such as flowcharts.

Where the answer to an ICQ is 'no', the auditor must decide:

- if this affects the operation of the system and the integrity of the data
- how this will affect the testing strategy adopted, for it is not possible to test a control that does not exist.

In some cases, the lack of an expected control may be compensated for by the operation of another control or number of controls ('compensating controls'). Auditors should always consider whether the compensating controls are adequate to address the risks identified.

Where controls exist, the auditor should record these on the system's documentation so that they may be considered as part of the overall controls when the system is assessed and the testing strategy is decided.

Where a major weakness is identified by an ICQ, the auditor will have to decide what action to take and how this result impacts on the overall audit objective and the level of any subsequent testing to be performed.

The auditor must document clearly why a control may or may not, in his or her opinion, meet a specified control objective or why a control weakness is not significant. This should be recorded on a 'record of control weakness or breakdown'

and cross-referenced to the ICQ.

Once the auditor has documented the system, he or she can form a preliminary opinion on the design of the system but will then need to form an opinion on the system in operation. This is achieved by testing the controls identified.

The ICQ is cross-referenced to the schedule of compliance tests.

Compliance Tests Papers

Each compliance test is cross-referenced to the relevant ICQ and broken down into the same sub-systems or procedures to aid risk assessment.

Compliance tests (tests of control) seek to provide evidence that the internal control identified as being in place is operating in the manner intended by management.

Where an error is found as part of audit testing, the error itself may not be that important – it is more what the error tells the auditor about the operation of the control. The precise nature of any compliance tests will depend upon the type of control being tested.

The level of testing is a matter of judgement, given all the relevant factors, and should take into account the result of previous audits so that known or suspected risk areas can be tested accordingly. The objective is to undertake cost-effective tests using appropriate sample sizes to obtain reasonable assurance that controls are functioning properly rather than spending excessive time that proves unwarranted. The selection of items to be tested is critical and needs to be based upon judgement or statistical sampling.

The schedule of compliance tests thus provides the auditor with a series of tests, cross-referenced to the specific controls to be tested, designed to enable the auditor to make a judgement on:

- the reliability of the controls and the integrity of the system
- the degree of reliance that can be placed upon the system
- the level, if any, of any substantive testing required.