A Modern Approach to I.S. Auditing

When looking at a "modern" approach, I do not believe I mean a "new" approach! The audit concepts, standards and practices I shall be expounding in this brief article are probably familiar to many readers. Perhaps, however, you will not have considered all of these issues together as a single methodology.

I believe audit practices are evolving to meet the needs of business, in the same way a business is evolving to meet the needs of customers and the threat of competition. My intention, therefore, is to stimulate thought about how we approach our work; about the relationship between auditor and auditee and how we, the IS Auditors, can bring a "value add" to our department.

Business is changing: there is no doubt about it. Business are subject to many cultural influences, many of which emanate from America and Japan; these are leading to changes in management concepts and practices to which we, the auditors, must respond. Many of the changes lead to obvious threats to the "audit universe" as they make it less evident who is in control, and who has responsibility for control. It is these implications that we need to address.

The traditional corporate structure is hierarchic. The Chief Executive, Managing Director, Chairman and so on have overall control distributed through Directors who are members of The Board to Senior Managers, Managers, Under Managers, Supervisors, Senior Staff and so on down. The responsibilities of each level are clearly defined and tend to be obvious, i.e. if you want to talk about "Sales Ledger Processing" then there is a clear line from the "Sales Ledger Clerk" through the Ledgers Manager to the Finance Manager and the Director of Finance (by whatever names they are known, they exist and their job description is clear) with any IS elements looked after by the IS Department.

Audits could be planned well ahead; the "three year audit schedule" was common. Not only could the Head of Audit identify specific audit entities, such as "Sales Ledger Processing", but could also identify the scope of the work in terms of management and staff. The people might change, but the job titles and duties remained.

Then what happened? Market forces demanded that the business react more speedily, more efficiently to customer demands, and the actions of main competitors forced business to comply in order to remain competitive. Technology, as we all know, is in a constant state of change, partly this is driven by the needs of business but it is also responsible for generating business changes in itself. There are many examples where market forces and new technological opportunities have forced major changes to business structures; consider the popularity of "Client Server" until very recently! A classic example, on which I shall base much of this article, is *Decentralisation*. This simple concept of devolving business responsibility from the centre of the organisation to local management is almost impossible to address using the "traditional" approach to audit.

Taking a step backwards for a moment, what is it that the modern IS Auditor needs to understand that in the past could be left to others? Simply it is the corporate strategy. IS Auditors must be aware of the business strategy, its "Mission Statement", its business objectives, priorities and guidelines. Also, how the IS Strategy supports and implements the business changes; how the Communications Strategy develops the future direction of the organisation and how all of these strategies affect the Corporate Structure.

Audit must be able to relate its activities directly to elements of the Corporate Strategy in order to be seen as an integral part of the business. To do this, we must ally our audit plans to meet the needs of the business – if this audit does not help the company to meet its strategic aims, then why are we doing it? We must be able to adapt our working practices to meet the changing structure; we must be flexible enough to react to cultural changes and, above all, we must address management concerns in addition to audit issues.

Returning to Decentralisation, which, as I said, is a classic strategic change. This concept is intended to empower local management to make decisions which would otherwise have been taken centrally; it often leads to a "profit centre" culture, where the performance of individual business units is assessed by their profit contribution to the organisation. Decentralisation is seen to take advantage of develop-

ments in information technology, to be flexible and reactive in meeting customer demands and fighting off the competition. In short, it enables a very large organisation to operate as many small businesses, operating locally, advertising locally and meeting the needs of the local market.

A typical comparison between centralised and decentralised structure would be:

Centralised	Decentralised
1 or 2 large sites	Multiple, small sites
Hierarchic management structure	Flatter, business unit management
Specific line management authority	Local autonomy to make decisions
Massive IS Department	IS Department acts as a support function
Systems developed centrally	Local applications development
Mainframe with LAN front end	Local mid-range system & LAN
Controls managed centrally	Controls managed at local level

Turning to the "new" audit risks generated by this type of organisation, consider the following as just a sample of the more obvious concerns:

- Small sites? Do they meet adequate physical and environmental standards?
- Flat management structure? Is there adequate management control?
- Local autonomy? Are local purchases cost-effective and compatible?
- IS as a support function? Waste of central resources which are often duplicated locally?
- Local development? Are control features included? Is effort being duplicated?
- Local hardware? Duplicated purchases? Duplicated business continuity? Physical and environmental security maintained?
- Local controls? Do they exist? Do local user needs take precedence over control requirements? Who has responsibility?

The net effect upon Internal Audit is that the audit entities are now having to be redefined. For example, when control was centralised, we would audit "Logical Security"; now such an audit may be spread over several sites and different departments. It is also more difficult to establish responsibility, yet it is essential that for each business unit we determine who :

- Ensures compliance with Corporate Strategy (as opposed to local objectives!)
- Manages and administers security, both physical and logical
- Controls adherence to corporate standards (assuming they exist!)
- Maintains management controls and other checks
- Maintains and co-ordinates business continuity plans

So, using decentralisation as our example, we need to adopt a modern, more flexible, responsive approach, less rigid than the traditional way; focused on strategies rather than "audit controls"; overtly biased towards the needs of the business. This can now be considered representative of all other forms of "new" management concepts.

Dare I say, we should promote an image of being positive and helpful, more consultants than policemen. Of course, changing our image carries with it the serious danger that we become too close to the business, and too close to the auditees! Then what happens to our independence?

Yes, I freely acknowledge that Internal Audit MUST at all times maintain overt and genuine independence otherwise reports cannot be seen as truly objective. If you are to provide the added value that should result from the modern approach, loss of independence is the most serious risk which must be carefully monitored and controlled. I failed in this area when auditing physical security of a site; having established the areas of weakness and convinced management of the need to address the issue, I found myself giving advice on re-siting cameras, purchasing new computer equipment and so on, which effectively prevented me from auditing the topic again – otherwise I would be, to a great extent, auditing my own work! So, consultants, please, but beware of giving too much detailed advice.

Take an holistic ("whole body") view of the business: examine the structure of the enterprise. Use the structure to compare and contrast business units and ensure corporate standards exist and are applied at the local level.

Be prepared to react to changes in the organisation and its technical infrastructure: the audit plan is still a valuable document, but it must be a flexible, "living" document which is

always focused on key, business risks and underlying threats, both appreciating and addressing the needs of business management.

Use CobiT (Control Objectives for Information Technology, ISACAF) to help you to establish control objectives for your organisation. You'll find that using CobiT in a risk-based approach helps you to relate to management at all levels – risk *should* be something they understand.

Consider your relationship with the auditees; I achieved great success when working in the financial sector by changing the department's name from "Inspection" (the traditional name for audit in a banking environment) to "Audit Services", a change of emphasis from policeman to service department. This emphasis must be followed through into the whole audit process, keeping auditee management fully informed of progress, especially as findings emerge. This will give management time to implement solutions leading to what I consider to be the best form of audit report which states "We found problems but the manager fixed them straight away".

Consider the form of the report. Auditors are often accused of negative reporting, failing to address business issues, reporting irrelevant issues and so on. If your audit objectives address only business issues, you ensure the auditee is aware of all the findings and recommended solutions in advance of the report, and you are positive in style, reporting good things as well as bad and giving credit where it is due then you will find your work becomes both easier and more productive as you gain the confidence of managers and staff. My own experience shows that being open and reasonable has led to managers approaching me with problems in advance of any audit work, knowing that I would help them find solutions not blame them for failures.

Why bother with examining your approach to audit at all? Surely Internal Audit is an established part of the business with rights of access to anything at any time, responsibility for reporting weaknesses and threats to the Board and/or the Audit Committee. Surely Internal Audit is untouchable? Don't you believe it!

In today's business enterprises, any non-productive area might be considered dead wood. Many companies have a definite policy of outsourcing anything not defined as "core" processing, which term, in most cases, does not include Audit. So what are the consequences of failing to address the "live" business issues and meet the needs of your specific business ?

- Audit Credibility may suffer and our findings discounted as irrelevant
- Audit may be marginalised and considered outside of the business
- Audit may be seen as unnecessary – not all organisations need the internal audit function or are required to have one by regulations
- Audit could be "down sized" addressing a much reduced audit universe of "key" areas only
- Audit could be outsourced; take it from me, there are many audit organisations who will claim they can perform the basic audit functions more efficiently and at considerably less cost than you.

This, then, is the need for internal auditors to provide the added value which comes with a detailed knowledge of the business and its objectives, a harmonious working relationship with the line managers and staff and a day-to-day visibility within the organisation … all of which will give you a distinct advantage over an audit "firm" which, by definition, remains outside the organisation.

To summarise, the modern approach to IS Auditing requires that you:

- focus on the strategic business issues and the needs of management
- adopt an holistic approach, auditing the organisation as a whole
- ensure corporate standards exist and are applied wherever control is devolved
- appreciate the risks and advantages of local empowerment and
- maintain a flexible audit plan to cope with technical and organisational change

I maintain that this approach will give you a more efficient, more effective more productive and more enjoyable job.

Derek J. Oliver is a Certified Information Systems Auditor, a Certified Fraud Examiner, a Member of the British Computer Society and a Freeman of the City of London. With over 16 years experience in IS Auditing during which he was in government service with HM Customs and Excise and led the UK audit group of the world's largest processor of credit card transactions, he is now Director of IS Audit & Security Consultancy for Ravenswood Consultants Limited. He is past-President of ISACA's London Chapter and is currently a member of the CISA Certification Board.