ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 5 NUMBER 2 AUTUMN/WINTER 94

The British Computer Society

Members' Meetings for 1995

17 January (3.30 pm for 4.00 pm start)	Joint meeting with the IIA-UK, Home Counties District **Business Process Re-Engineering and Its Impact on Internal Controls, with Examples**	Peter Adams Adams Training & Advisory (formerly UK BPR Manager, DEC)
14 February (full day) Contact: Bill Barton 01883 623355	Discussion Group **Runaway IS Projects** (see inside back cover)	
14 March ICAEW, Moorgate Place London (4.00 pm for 4.30 pm start)	Joint Meeting with the IT Faculty, ICAEW **Unix Security** Please inform Margo Ellis, ICAEW on 0171 920 8481 if attending	Steven Duke RAXCO
4 April (4.00 pm for 4.30 pm start)	Joint meeting and debate with ISACA London Chapter **Debate - Topical Motion**	Speakers to be announced
10 May (full day) Contact: Jim Ewers 01992 555328	**Discussion Group**	Speakers to be announced

Meetings are usually held at the Royal Institute of Public Health & Hygiene, 28 Portland Place, London W1N 4DE, except as noted above. For last minute confirmation, telephone the RIPHH (0171-580 2731 or 0171-636 1208). Meetings start at 4.00 for 4.30pm, unless otherwise stated. Tea and coffee are available before each meeting; sandwiches and refreshments afterwards.

Details of discussions groups are forwarded directly to members as part of the quarterly mailing. Please contact the relevant organiser for further information.

IS YOUR SUBSCRIPTION DUE? - See page 12

FEBRUARY 1995 DISCUSSION GROUP – SEE INSIDE BACK COVER

IN THIS ISSUE

LETTERS TO THE EDITOR

are welcome, write to:
Rob Melville

Centre for Internal Auditing
City University Business School
Frobisher Crescent
Barbican Centre
LONDON EC2Y 8HB
Fax: 0171 477 8880

Editorial

Beginning with this issue there are some significant changes to production of the journal. We have arranged for all of the production tasks - typesetting, layout, printing and distribution - to be taken over by our typesetters. This means that the weakest link in the editorial chain has now been strengthened. In four years editing the journal this has been without any question the area where volunteer labour is hardest to find; authors and critics, no problem. Finding someone to stuff five hundred envelopes with mailshots and journals? A different story! Luckily my students were usually amenable to carry out this task for a few pounds, but more than once my office floor has been filled with the papers for members. Outsourcing production has also been the final part of the journal's processes to be professionalised. The editorial team will now be able to concentrate on issues such as content, style, and quality. This naturally leads to a need to address the editorial committee and its role. For us to maintain its present status as probably the best specialist journal, we need to relaunch the editorial team.

The new team must be able to give expert advice on current issues in computer auditing, and to encourage potential authors. Having already set the precedent of publishing refereed papers (the next one should appear next issue) we need a refereeing panel. In addition, specialists are needed in:

- the law and computing
- CAATs
- networks
- databases
- emerging technology
- the internet
- client server systems

and many others. If you want to review books and software, or just quality assure articles, your support will be gratefully accepted. And finally, just because the editorial chair has been my fief for so long does not mean it would not be relinquished if a better candidate came along. Any aspiring hack should call me if they are interested.

* * * *

Recently *The Independent* carried a story which must have made them think Christmas had come early. An imaginative young hack(er) had managed to combine royalty, hacking, the internet and a privatized industry in one story. Apparently the journalist had gained confidential telephone numbers from BT's database using the Internet. Superficially it was a plausible story: advertise your interest on the 'net, then wait for the gory details. The story's only letdown was the omission of downloading GIFs of naked royalty via the hacked telephone numbers. But any reasonably cynical audit professional would have seen the holes in the story. Of course there are people on the Internet who have access to this information, many of whom are willing to share. But a committed 'netsurfer' would realise that breaking into these groups is not easy, they like to check out credentials first.

My first thought (having worked at BT as a temporary for a time, years ago) was that he'd probably worked there himself and just grabbed the information for himself. This is not a criticism of BT, whose security practices are at least as effective as any other major plc. But systems have to be used, and the small minority of information thieves and abusers must be balanced against business efficiency. My advice to *The Independent* is sack the devious little sod and start concentrating on real stories.

Continued over page

NEXT DISCUSSION GROUP

SUBJECT: Runaway I.S. Projects

DATE: Tuesday 14th February 1995

Despite forty years of developing computer systems many projects still come in late, are over budget and fail to meet the user functionality requirements. Why is this so and can audit help to tip the scales from failure to success? This discussion group will have leading speakers, including Paul Williams from BDO Binder Hamlyn and representatives from Hoskyns and two other leading I.S. consultancies.

SPACE LIMITATIONS: As usual we will be restricting the size of the group to twenty members in order to maximise the discussion aspects. Place allocation will be on the usual first booking, first allocated basis. The last discussion group was over-subscribed by more than fifty percent and we had no option but to refuse late bookers, so act quickly to reserve your place for this valuable training day.

FURTHER INFORMATION AND BOOKING: Due to the popularity of these events there will be no further notification to you regarding this one, so don't put it to one side to be dealt with later, as you may find that later is too late. Contact the organiser now!

Bill Barton
Senior Audit Manager
The Rank Organisation Plc
439-445 Godstone Road
Whyteleafe
Surrey
CR3 0YG

Telephone: 01883 623355
Fax: 01883 626044

Contents

Chairman's Corner

John Mitchell

As both chairman of this group and someone who does a bit of post-graduate lecturing I am used to receiving requests along the lines of 'could you please let me have everything you know on computer audit and control for my forthcoming ..... thesis, board paper, audit report, annual plan, etc.'. The really sad thing is that in most of these cases the person making the request does not even understand basic computing, control concepts, or audit techniques. I had just such a request a few days ago and it quickly became apparent that the person on the other end of the line had simply contacted the BCS for information on computer audit. Well, at least that is a sensible start, but it then turned out that they knew nothing about the various standard text books on the subject. Well, everyone has to start somewhere, but it was the response to my question 'who is responsible for computer audit in your organisation?', that really showed me just how deep the problem was. The response was 'I am', followed by, 'I just thought I'd bone up on the subject so that I can do one of these risk analysis things that I've heard about'. When I pointed out that in order to conduct a risk analysis, one had to be able to identify and understand the risks, the response was, 'That is why I am contacting you'. When I suggested that they may wish to consider getting in a consultant to help them, the response was, 'No, I think that we can do this ourselves'. At what cost I wonder?

So, in order to help budding young control experts Rob Melville, the editor of this Journal, and William List are publishing the executive summary of their recent paper on I.T. control. This provides a good starting point on the subject and you can always buy the full copy for your bookshelf. I know that the full paper is good, because I refereed it!

* * * *

The BCS has overcome its financial crisis and is now really beginning to motor! The publication of details of the various specialist groups has brought in a number of enquiries from potential members. On its own side the BCS claims to have speeded up the processing of membership applications and is currently updating its 'Industry Structure Model'. The ISM is a useful, if somewhat expensive publication, which attempts, and I believe succeeds, in mapping the various IT jobs and skills against each other. My only concern with the last edition was that Information Systems Audit was shown as being 'non-core' to the IT process, whereas so called 'quality auditing' was considered to be 'core'. It was also shown as being graded higher for equivalent jobs (i.e. senior auditor) than the IS Auditor equivalent. I am currently batting for our side on this one, so that we can get the anomalies corrected for the third edition. 'Why worry?', you may ask. Well, it could have direct implications for your status in the organisation and thus your pay cheque! I will keep you informed of progress.

* * * *

We still have problems in persuading people to submit articles, letters, book, or product reviews to the Journal. A couple of times, the editor and myself have discussed the offering of inducements, but such as been the poor response to such things in the past, such as the appalling response to the group's last survey, that we have decided against it. Does this general level of apathy indicate an alarming lack of interest amongst UK computer auditors? I regularly receive copies of Journals from our sister groups in the USA, New Zealand and Australia and they are packed with contributions. One of our members commented in the last survey on the content of the Journal, 'Only one major article, is the CASG dying?'. Well, it will unless you, the membership, positively support it. Get that word processor fired up now!

Editorial - continued

Ever heard of 'netiquette'? This is the voluntary code of practice for 'net users, and covers things like how you use the service. Offenders are 'flamed', that is, sent hard hitting messages if they transgress. My university staff association sent an experimental email to all members, to which I replied. Unfortunately I did not specify that only the source should receive my reply and the response (about two short lines) was sent to the group. One irate recipient took the trouble to point out the error of my ways, telling me about the wasted time reading messages that were misplaced and confidentiality issues and so on. This flame without question took longer than a simple 'delete message' would have, and instead of enlightening me simply served to create an irrational anger at the type of anorak-wearer who feels the need to electronically moralize. So for him, and any other netsurfer who feels the compulsion to police the system, get a life. If you can't do that, get a delete key! A very happy Christmas and a prosperous new year to all of our members.

ROB MELVILLE

Integrity in Information Systems

Executive Summary

William List CA FBCS and Rob Melville BA MA MBCS MIIA

IFIP WORKING GROUP 11.5

June 1994

International Federation for Information Processing (IFIP) Working Group 11.5 addresses 'Systems Integrity and Control' within the overall remit of Technical Committee 11 (TC11) 'Security and Protection in Information Processing Systems'.

This paper was previously published in *Computers and Security.*

Section 1: Introduction and Background

Objective of the project

IFIP Working Group 11.5 undertook a project to determine if the existing guidelines and standards used by IT practitioners, users and auditors were adequate for future system trends. We used as a starting point for our project the fact that users make decisions based on output from computer systems. Clearly if the output is wrong there is a probability that the decisions made will also be wrong. We therefore adopted a definition of integrity which was appropriate for a user:

> 'Information is sufficiently right at the time of use for the purpose to which the user wishes to put the output.'

The indications are that future systems will comprise large networks containing distributed data and that the information supply will be largely user initiated. The present trend for business process re-engineering is encouraging the development of such systems.

As in the past, the existence of errors in information provided from systems may well lead to loss of confidence by users or the general public, thereby inhibiting the full benefits of such systems from being realised.

Integrity and Controls as Presently Conceived

IT Community

Generally accepted systems development procedures include integrity requirements. These encompass both the need for the systems to meet business objectives and provide required information to appropriate users as well as detailed integrity requirements for input validation, full and thorough testing of programs and systems, etc.

The Clark Wilson paper and subsequent discussions postulated that the solution to IT security/ integrity was dependent upon:

- trusted computer base;
- trusted procedures;
- trusted processing;
- authenticated procedures and audit trails; and
- segregation of duties.

This narrow view of what constitutes integrity is confined within the logical bounds of the IT systems. It excludes the material impact of the people and business application processing necessarily involved in any system.

Accounting and Auditing Community

It is a fundamental view of the accounting and auditing professions that management at all levels are responsible for the performance and control of their organizations. This has recently been highlighted by the reports on corporate governance published in the UK, Canada and the USA.

Management create Internal Control systems to discharge their supervisory and other responsibilities.

Responsibility and Trust

Areas which are particularly pertinent to integrity and the creation of Internal Control structures discussed in the material are the concepts of responsibility and trust.

Senior management of organizations (inter alia the board, or their equivalent) are ultimately responsible for the integrity of their systems. A fundamental principle of Internal Control is that a system provides the capability to enable delegated staff to be supervised. Whilst the extent of active supervision may vary depending on the task and the level of 'trust' vested in the person(s) or process(es) performing it, some supervision will always be required.

The concept that a system can be trusted over time without the ability to provide the evidence that the trust is well placed is incompatible with Internal Control principles. The concept of trust therefore is insufficient for our purposes.

Assumption of Integrity

We wished to establish a basis for our replacement for the concept of trust in the context of the practical systems environment where:

- most people now assume computer systems and processing to be right unless it is clearly not the case, without any evidence whatsoever; and
- it is uneconomic for evidence of integrity of all data/software to be provided at all times to all users irrespective of their needs.

We define this state as 'the assumption of integrity'. To conform to Internal Control principles the assumption of integrity must be capable of being demonstrated to be true.

If the assumption of integrity is to be demonstrated to be true, it will be necessary to decide:

- which elements within the system are germane to the integrity objective;
- how often should the demonstration take place, and
- how thorough should the demonstration be.

The exact needs in relation to any one specific system or piece of information can only be determined in the light of specific circumstances.

It must always be remembered, however, that:

- it is unacceptable never to be able to demonstrate the assumption of integrity to be true; and
- it should not be a general requirement to justify the assumption of integrity on all occasions.

The study team sought to identify the extent of the potential elements within a systems which could be considered germane to the integrity objective and therefore potentially targets for a demonstration of the truth of the integrity assumption. These elements we have referred to as 'integrity components'.

Integrity Components

General

Figure 1 represents the overall structure within which we considered integrity components. On the left of Fig 1 we have shown the flow of assumption of integrity. Each component is dependent upon the proper functioning of the component below it in the core column, yet it is possible to so construct a component that any failings in prior components can be mitigated by provision of compensating controls or information on the extent of integrity failures in a subsequent component.

As a contrast, Figure 2 represents the traditional IT view of security which relies on a Trusted Computer Base and control over input.

Information Users

Information users are the recipients of the information. They must therefore be able to judge if the information is 'sufficiently right at the time of use for the purpose which they intend to use it'. If they are unable to make the judgement the possibility of wrong use of information exists.

The correct information user should receive well presented information at an appropriate time for use. Inappropriate presentation of otherwise perfect information may lead to misunderstandings and wrong decisions being made.

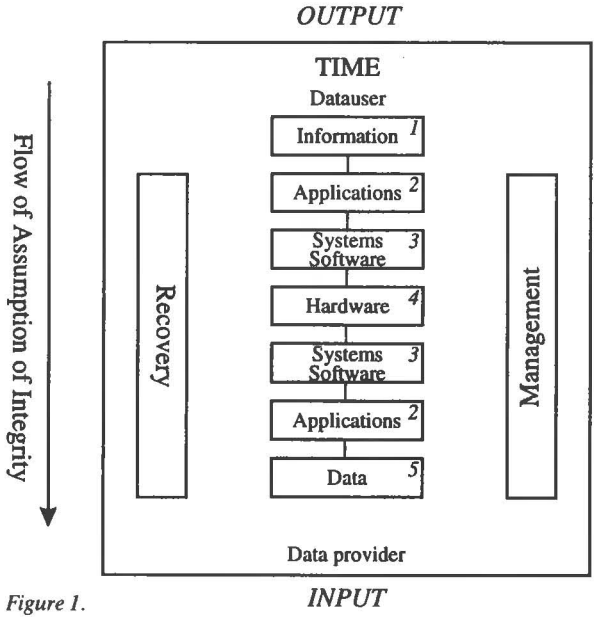


Figure 1.

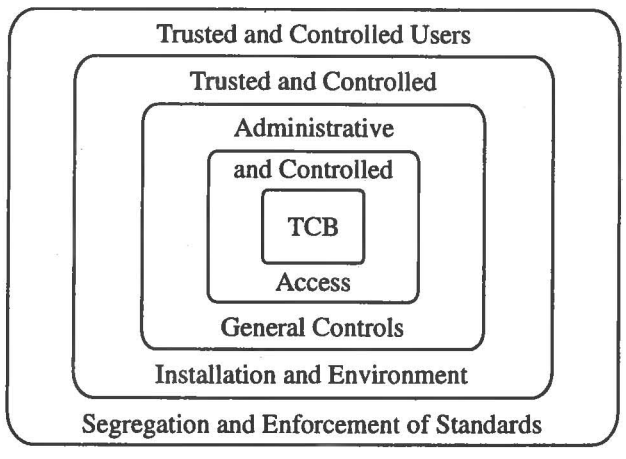


Figure 2.

All data users should be supervised to the extent necessary and comply with any Quality standards in place in the organisation.

Information Provided

Information may be generated either by specific (ad hoc) request, probably by the information user in an End User Computing environment, or as part of a regular predetermined processing (Application system).

In either circumstance the need is for the extract to be

- complete;
- made from the correct and complete data appropriate to the information; and
- created by appropriate and correct software.

Additionally if the information user is making the request then the translation of the request into the specific instructions required by the extraction software must be correctly and exactly stated.

Applications

Fundamental to the integrity of applications is the requirement that processing by application software meets the business requirements. If the processing by applications is not as expected by the information user then it is likely that the information user will misinterpret or misunderstand the information provided thereby leading to misunderstanding.

We have divided our consideration of applications into three parts: Development, database and use.

Development

We believe that the generally accepted system development procedures will largely meet the requirements in this area, provided they are followed thoroughly. The problem is that systems rarely demonstrate to the information user that integrity has been maintained.

Database

This area is concerned with the specific problems relating to the capability of a information user to clearly understand the data elements which can be accessed to meet the information requirements. If the information user is unclear as to what data items represent or which data items are available, then it is likely that the information user will be unable to be satisfied that the information from the system meets the integrity needs.

Use

The use of the correct application software applied to the correct data is fundamental to maintaining integrity. Procedures should exist to demonstrate that this was the case.

In many modern systems parameters are used to govern the exact performance of application software. We believe that the ability of a user to confirm that these parameters are correct is important in maintaining integrity.

Systems Software

Systems Software in our classification covers all the general nature software necessary to run specific applications. We have identified operating systems, the database management system (DBMS), the teleprocessing monitor (TP monitor), compilers, utilities and access control software as representative of this class.

The proper functioning of the whole system is dependent on the proper functioning of the base systems software. Today systems software is usually purchased, often from multiple vendors. A primary requirement is that the systems software functions with the other elements of the software, the hardware and the applications so that errors are not introduced.

This software contains many functions which, if used improperly, could cause substantial damage to data and software.

Hardware

In writing this paper we have assumed that the hardware in use in any organisation is configured to meet the business requirements. This gives rise to a multiplicity of structures which render the traditional descriptions of mainframe, minicomputer and PC open to misunderstanding by readers. We have therefore not sought to describe the components in detail.

Physical hardware is basically reliable and breaks down infrequently. Failures in communication systems are more frequent particularly over long distances.

If through malfunctioning the hardware causes an integrity failure in the stored data then it is our contention that this should be capable of detection through the application software. It is important however that failures of hardware are detected promptly and recovery effected as soon as possible after the event.

Data

Data is supplied to user applications and to systems software/hardware. It is this data which both governs the specific operation of systems and records the events of an organisation. Data may originate from people (data providers), be generated by the system or prior application processing and may originate both within an organisation or be imported (possibly via telecommunications) from external sources.

Data provided to systems will have specific integrity attributes at the time of input, or generation. These attributes will include the quality of the data itself (for example: exact, best estimate, draft document etc.) and the time of creation or input/ generation. The information user should be able to access these data attributes to assist in judging whether the data is sufficiently right for the purpose to which it will be put.

Data is classified in this project into four groups, based upon the permanence and pervasiveness in the processing. These classes are:

- Parameters: data which governs the operation of application or base systems software. This data is specific to the operation concerned and is usually unchanged over long periods of time.

- Standing data: data relating to specific activities (eg a name and address) which is subject to infrequent alteration. These activities are in the users' domain.

- Tables: data relating to specific activities which is held for varying lengths of time. This class of data does not necessarily relate to the physical data structure which may occur in certain databases.

- Transaction: the unit of entry or creation of data which represents the whole or a part of a single real world event.

In our view an essential part of the capacity to demonstrate that the assumption of integrity is true is the ability of users to confirm the correctness of parameters, standing data and tables at appropriate intervals. Software using parameters, standing data or tables should also include tests to demonstrate that this data and the transaction data being used in a process are time consistent and up to date.

Input

The input of data is either:

- Creation of a new data entry (including copying of an extant item) or

- Amendment (amend/delete) of an existing entry.

Generated data - Applications

Generated data is new data created from existing data; it may be amended by input of data. Procedures to demonstrate the completeness of the creation of the generated data are essential.

Generated data - Logs

We have treated all logs created by systems software, or applications as generated data in our model. As with the generated applications data, procedures to demonstrate completeness of the creation of the required logs are essential.

As the logs contain, inter alia, the record of the system events there should be software available to allow a non-technical person to understand what happened, in order to assist them demonstrate that the assumption of integrity is true.

Storage - Continuing Correctness

In theory, once data is input and stored it should never become corrupted; in practice the possibility of corruption exists. Procedures must therefore be established to detect any corruption.

Storage: Databases

Data may be organised in databases to suit the requirements of particular processing. In certain cases data elements occur more than once, for example summaries of data elements are held. Part of the capacity to demonstrate that the assumption of integrity is true is the proof that the multiple storage of data is in itself both complete and consistent.

Archive

Once the stored data has become history it is Archived. Procedures should exist to demonstrate that no corruption has occurred to the data in its archived state.

Data Providers

The last element of the core of our model is the data provider. The data provider is a person at any level within an organisation who may also be the data user (for example where a person creates and uses a spreadsheet). If data is automatically transferred from another system then a person should be in a position to confirm that the data provided is fully appropriate.

Much of routine data input is performed by junior members of staff; adequate procedures must exist to supervise their work.

Recovery

When applied to integrity, 'recovery' is a pervasive activity, applicable to every element within the system cycle. Anything may go wrong at any time, and recovery may be necessary so that systems can continue to function. During recovery the routine processing is disturbed (or possibly suspended); this break in routine is itself a threat to integrity and necessitates the establishment of procedures to demonstrate that the recovery process has resulted in an integral system and associated data files.

In addition, it is also necessary to ensure that on restart of normal processing no transactions were

missed, duplicated or corrupted. Where recovery is spread over a prolonged period of time it may be difficult to establish this.

Time

A critical element for our definition of assumptions of integrity is time. No information system is ever 100% up to date in relation to real world events. Input to systems is governed by clerical processing cycles; computer processing is performed to time cycles with certain processing being performed at specified times; detected errors are corrected to different cycles and the elapsed time between detection and correction will vary. All these differing cycles will result in the data never being at a consistent point in real world time.

Any incompleteness, in relation to the user's perception of time, in the data used to create output may render the information insufficiently right for the purpose to which it is to be put. It is also possible that output created at different times which purports to represent the same event(s) may give differing results. This can cause confusion to the users.

Communications

All transmissions require technical compatibility between the parties and the ability to determine that the transmission is with the expected party.

Procedures should ensure that transmissions received are acceptable to the recipient before they are used as input to applications; in other respects they should be treated as any other input. Other procedures should exist to confirm that the transmission from an organisation is as expected and that no corruption has been introduced during the translation and transmission process.

Management

Management is a process which has responsibility for ensuring that specified tasks are performed. It comprises many organizational levels from the board to line management. Senior management set policies for other staff and automated functions to follow in order for specified tasks to be accomplished. Management therefore has a duty to supervise delegated tasks to ensure that they are carried out to a satisfactory level; the systems in an organisation should be designed to assist management to perform their duties. In relation to Integrity we believe that this includes:

- the ability to demonstrate, when required, that the assumption of integrity is true
- provision of functionality in systems to assist information users in determining on a day to day basis that the information they are receiving from the system is sufficiently accurate for the purpose(s) to which it is to be put

Conclusions

The definition of integrity as 'information is sufficiently right at the time of use for the purpose to which the user wishes to put the output' encompasses all the major integrity requirements in any system. Therefore, this should become the overall integrity definition used in security and control discussions; other definitions should be put into this overall context to aid understanding.

In the vast majority of situations information is assumed both by software and by people to be sufficiently right. This assumption has been defined by us as the 'assumption of integrity'.

It is unacceptable in the context of Internal Control theory to rely on assumptions that cannot be justified. System designers and users must therefore ensure that the capability to justify the assumption of integrity of information is provided by the system.

In future systems the functionality to provide the users with integral information will be vital. This will require changes to the present codex of standards and guidelines in both the IT and accounting/auditing communities.

IFIP WG 11.5 will continue to explore the concepts of integrity based on our work to date. We look forward to receiving comments on this paper to assist us in continuing our research. ■

Copies of the full paper are available at £25 Sterling. (Payment in other currencies should include an additional £3 translation charge).

Please contact Rob Melville at City University Business School, Barbican Centre, London EC2Y 8HB England. Tel. 0171 477 8646, Fax. 0171 477 8880, Email SC355@CITY.AC.UK

VFM Auditing in an I.S. Environment

John Mitchell

INTRODUCTION

This paper will examine Value For Money (VFM) from two separate, but related, viewpoints: the ***common sense*** approach and the ***measurement*** approach.

The common sense approach would be recognised by any prudent person; how can I either save money, or use the product that I already have more wisely? The measurement approach is more akin to management accounting and deals with standard setting, attainment and the explanation of variances. The questions to be answered in this case are; what is a fair standard and how can I measure performance against it?

The common sense approach can easily be applied to any data centre on a good housekeeping basis, but it does present problems when attempting a comparison with a similar service elsewhere. The measurement approach, although more "scientific", is fraught with the problems of setting the standards in the first place and then implementing a system to obtain the metrics for comparison. Both approaches suffer from the problem of determining what is fair and equitable for the service in question.

WHAT IS VFM ?

Value for Money concerns itself less with the application of management directives and more with the efficient, economical and effective deployment of resources. It has nothing at all to do with doing things on the cheap!

From a management viewpoint, conducting a VFM review can be very stimulating, as the manager is not constrained by existing policies, or directives; rather he should be taking a completely new look at an area of the business. On the other hand there is the danger that reviewer will visualise himself as the saviour of the organisation, but without the responsibility of implementing the recommendations!

THE THREE "E's"

Although the three "E's" are usually understood in concept , I will define them in the way that they are used by the UK's National Audit Office, which is well experienced in VFM work.

Efficiency is concerned with the relationship between the output of goods, services or other results and the resources used to produce them.

Economy is concerned with minimising the cost of resources acquired or used, having regard to appropriate quality.

Effectiveness is concerned with the relationship between the intended results and the actual results of projects, programmes or other activities.

Basically, **Efficiency** is about achieving maximum output for a given input (spending well), **Economy** is about spending less and **Effectiveness** is how successfully does output of goods, services or other results achieve policy objectives, operational goals and other intended effects (spending wisely).

There are a couple of other "E"s which are becoming important. These are "Equity" and the "Environment", but I shall not be dealing with these in any great detail in this article.

VFM AND QUALITY

Someone can always produce something cheaper, but it doesn't mean that it will be as good, or last as long, as the more expensive product. There is a danger that an incorrect application of VFM principles could actually be counter productive if the longer term is not taken into consideration. For this reason it is essential to establish whether there is an appropriate British Standard Institute (BSI), International Standards Organisation (ISO), or other standard which is applicable to the area being reviewed as this will provide the appropriate base point for measurement purposes.

EQUITY AND THE ENVIRONMENT

A VFM review, like any other management review, should have defined boundaries, but it is essential to ascertain whether any changes to the system will have undesirable knock-on effects in other areas. As an example, money may well be saved by eliminating a computerised check over water purity, but if the environment then becomes polluted as a result, the organisation may well face expense statutory penalties.

The UK British Standards Institute, under a Royal initiative, have recently created BS 7750 to cover environmental matters.

The importance of these additional areas are only just being recognised and as more computer systems come into existence to control industrial processes, the manager will need to take more note of this area than has hitherto been the case.

VFM AND POLICY OBJECTIVES

In the past top management have not been used to having their policies reviewed!

With VFM however, it is often necessary to

evaluate the merits of policy objectives as a means of deciding on their ultimate effectiveness. The areas that need to be considered include:

a) the accuracy, reliability and completeness of the information provided for determining policy objectives and deciding on the means of pursuing them;

b) the clarity with which policy objectives have been defined and communicated to those responsible for implementing them;

c) the appropriateness and consistency of lower level operational aims, targets and priorities;

d) the systems and arrangements for monitoring results and achievement against objectives and taking appropriate action;

e) the consequences of any side effects of the policy, or its implementation.

CONDUCTING A VFM REVIEW

A VFM review normally consists of two distinct stages:

a) an initial study to establish whether and how the work should proceed;

b) an in-depth examination leading to a report.

There may be many more of the former, than of the latter, as not every investigation will proceed beyond the initial stage. This is because the subject matter may be found to be of insufficient merit for a full investigation. Thus, the initial "analytical review" is an important and essential pre-requisite of any VFM review.

As with any other review, the standard sequence of events ranging from objective setting, through to reporting should be followed with appropriate professional standards being applied.

Where possible, it is highly desirable that someone from the section, or area, being reviewed should be involved, as they will be able to provide local expertise and background knowledge which will help in the production of the final recommendations. Do not neglect to also pick the brains of people in other organisations, as they may raise issues that you would never think of!

SOME IDEAS FOR ACHIEVING VFM

The following "bullet points" are a guide to some of the areas that need to be considered in obtaining VFM. In some cases the suggestions will seem to be mutually exclusive. The point here is that all options should be considered for a particular situation and then the most cost effective solution should be chosen.

The Basics

- Understand your business and its objectives
- Ensure that everyone knows the objectives and how their job fits into the scheme of things
- Prioritise all activities to meet the business objectives
- Drop projects which do not link with those objectives
- Improve communications between IT and the rest of the company
- Obtain a knowledgeable and trusted external adviser

General Points

- Reduce in-house maintenance
- Get competitive tenders from outside
- Read the small print
- Treat feasibility studies as a cost
- Review R&D budgets
- Introduce new technologies slowly
- Make it difficult to spend money
- Instigate regular housekeeping checks

Purchasing

- Check the additional costs
- Buy at the right time
- Query all purchase requests
- Have a purchasing policy
- Reduce the number of suppliers
- Adopt open systems

People

- Develop a people policy
- Impose a head count freeze
- Encourage internal recruitment
- Implement a training strategy
- Pay people more
- Work people harder
- Use Contractors
- Reduce layers of management
- Limit Overtime
- Use Publications

Hardware

- Buy what you need and not what your supplier wants you to buy
- Rightsize
- Sell unwanted equipment
- Keep track of all equipment
- Use the right storage devices

Software

- Don't re-invent the wheel
- Use structured methods
- Use CASE tools if you know how to do so properly
- Use software cost estimation methods
- Trace requirements to deliverables and back again
- Manage projects properly
- Re-use code
- Take a modular approach
- Prototype whenever possible
- Use structured walk throughs

Operations

- Analyse the network topology
- Automate operations
- Solve problems remotely
- Analyse communications costs

Efficiency

- Measure and analyse performance
- Only use consultants if you are prepared to act on their recommendations
- Cut out duplication of functions
- Make maximum use of all resources (hardware, software, staff)
- Integrate
- Standardise ways of working
- Enforce standards
- Automate
- De-skill activities
- Push functions out to the users
- Set up information centres
- Implement a standard user interface
- Have a quality policy
- Measure productivity
- Know who is in charge
- Keep it simple
- Keep it Small

WHICH AREAS ?

The cost of IT to organisations has been rising as it moves away from the traditional operational areas of payroll and finance into the more exotic areas of front office client service. As a percentage of operating costs it is often quite low, but it has high visibility because of management expectations. Hopes that have often been let down with new systems coming in late, over budget and not delivering what is expected. While existing systems are faced with a backlog of maintenance and poor real-time response times.

The previous section highlighted some ideas for achieving VFM. The following examples are some of the areas that the author has investigated during the last decade, but it should be stressed that as every organisation is different, what is a prime VFM candidate in one company, may not be suitable in another, so remember to do a preliminary investigation before getting stuck in!

Micro Computer Maintenance

The organisation had a policy of always taking out a maintenance contract for micro computing equipment. Typically, this was ten percent of the gross cost for the first year, thirteen percent for the second year and seventeen percent for the third year. Maintenance after the third year was not available.

The reviewer first queried the fact that the maintenance charge was based on the gross cost, which included VAT and secondly why was the organisation paying for maintenance in the first year which was covered by guarantee anyway?. The reviewer then looked at the various fault logs which were maintained by each department and noticed that the most common failures were associated with floppy diskette drives and hard disks. A change of disk drive, conducted by a local company on an ad-hoc basis, cost in the region of £50 - £500, depending on type, and the failure rate per machine was only about every four years anyway.

Impact printers failed more regularly than their laser cousins, but again the cost of repair was usually less than the maintenance cost.

It was recommended that maintenance contracts should **not** be taken on micro computers, thus saving the organisation some £20,000 per year.

Mainframe Equipment Maintenance

An analysis of invoices for routine maintenance of the mainframe computers, coupled with an analysis of the fault log revealed two very interesting things. Firstly, the organisation was paying for 24 hour maintenance cover even though it only operated for 16 hours a day. Secondly, their were more machine failures in the first shift period just after routine maintenance than in the other periods.

It was recommended that the emergency cover was reduced to 16 hours per day and that routine maintenance was discontinued. The first point was accepted and the second was rejected on the grounds that routine maintenance was built into the contract and therefore had to be done. The saving on the first recommendation was in the region of £750,000 per year!

Software Rental

An analysis of the software available on the mainframe computers revealed old versions of operating systems, database management systems and many utilities that were never used. The old versions had been retained in case there was a need to revert to them when the new version had been installed. The situation had never been reviewed however and rental was still being paid for the obsolete software. The subsequent saving to the organisation was some £40,000 per year.

Software Purchase

There was no co-ordinated purchase plan for micro-computer software, with the result that the full retail price was being paid in many cases. A VFM review resulted in a "call-off" contract being established with a major supplier which showed savings of nearly 60% in the first year of operation.

A VFM review on the software purchases themselves revealed that only about 20% were being used on a regular basis by the purchaser!

Training

It was found that there was no strategic training policy for the IT staff with the consequence that training was conducted on an ad-hoc and often untimely basis. Staff were often mystified as to why they had been selected for training and disappointed with the course they attended. Feedback on courses was minimal and often unsatisfactory courses were used again.

The reviewer recommended that a complete strategic training methodology to match required skills against those already available in-house and which delivered skill acquisition to those that needed it at the appropriate time. No direct monetary savings were envisaged, but a more effective use of training resource was achieved which made better use of the training budget.

Mean Time Between Failures

An analysis of failure logs revealed that a particular peripheral, an OCR scanner, was particularly prone to breakdown and took a long time to get back on-line. It turned out that the reader had been obtained second-hand and at a good (i.e. low) price. It was costing more in down- time than it was worth and the reviewer recommended that it should be replaced.

System Maintenance Backlog

A preliminary analysis showed that there was a five year backlog of outstanding maintenance on existing systems. Most of the outstanding work was of the "enhancement" variety and a more in-depth review indicated that about 20% of these enhancements would result in a much better "front office" service to the organisation's customers.

A prioritisation review methodology was implemented whereby the backlog was reviewed on a quarterly basis, with contract staff being used, where necessary, to implement those enhancements that were considered to provide added value to the company. As a result of this regular review it was also found that many of the items on the list had been superseded by changes in working practices. This in itself resulted in the backlog being reduced by some two years.

Service Levels

This is often the heart of any VFM review of data processing. Is the end-user getting the type of service that they consider to be acceptable and what should that level be anyway? Many organisations now have service level agreements (SLAs) between the IT department and the end-users, but in some cases the SLAs are so badly constructed that almost any level of service can be explained away. The heart of many SLAs relate to the real-time response time and the availability of the network.

One SLA stated an average response time of three seconds and an average availability of 98% over a 24 hour period. Now the users only used the network 9 hours a day, but the averages were always calculated over the full 24 hours. The data centre could always meet its specified service levels, even though the peak-time response to the user was often in the region of 20 seconds!

Another organisation's proposed SLA stated that response time of under a second would be the norm. In order to achieve this the IT department requested expenditure approval of several million pounds for more powerful CPUs and communication lines. Discussion initiated by the reviewer with the end-users, revealed that a peak-period three second response time would be acceptable. The company saved itself many millions as a result.

Machine Upgrades

Sizing is a black-art at the best of times, so look very closely at what is being proposed. Does the sizing equation take into account the development and implementation of new systems as well as the natural growth of existing ones? Has consideration been given to the MIP consumption of likely new base software, such as the OS, TPMS and DBMS. Sometimes the IT people under-estimate the likely requirement and actually propose a machine that will too small, too soon. Occasionally, it is better to spend more now, than to repeat the exercise in the near future.

Communications Cost

The Leeds building society in the UK recently received a refund of £200,000 from BT for the rental of lines that were not required, but which had been recommended by BT. Just how much use does your

organisation make of privately leased lines? Sometimes an analysis can be revealing. One company had its own line to Egypt which was hardly used. It had been obtained at a time when a promising contract had been forthcoming, but the contract had never materialised and staff changes meant that the existence of the line had been generally overlooked. The company saved itself £17,000 a year as a result.

Facilities Management

The company had gone out to tender for the FM of its total IT requirements. The internal IT department was also allowed to tender for the job. The internal price was some thirty percent below than the next lowest tender. A VFM review established that the internal IT department has under-estimated their costs by some twenty percent! Although it was eventually agreed to give the contract to the internal IT department the organisation had a far better understanding of the cost of its IT operation.

Disaster Recovery

One organisation spent many millions on a hot-start standby centre capable of taking the largest of its many data processing centres in the event of disaster. A VFM review revealed that the software at the standby centre had not been kept up-to-date with the other centres. The money spent was effectively wasted, as the standby centre would not have been able to fulfil its role.

The outcome of the review was the establishment of a procedure to keep both installations in line with each other. Although this actually cost more money than had been budgeted, it was considered that this was the only way that the original intention of the standby centre could be realised.

CONCLUSION

The actual conduct of a VFM review is actually no different from any other in-depth review. The difference is usually in the preparation before the review commences, which often means that many potential reviews are never carried out in full, as the preliminary work indicates that a full scope investigation will not in itself provide good value for money! ■

John Mitchell is Managing Director of LHS - The Audit & Control Consultancy. He is chairman of the British Computer Society's Computer Audit Specialist Group, a visiting Professor at the University of Luton and a regular contributor to international conferences and journals. He can be contacted on +44 (0)1707 654040.

Membership Renewal

Some of you reading this edition of our Journal will not have renewed your subscription for the current season (subscriptions are due in August of each year). Others of you may be unsure whether you have renewed, or not. If you are in this last category, please contact our membership secretary, John Bevan on 01992 582439 to establish the current situation.

If you have not yet renewed your subscription, I urge you to use the renewal form that you will find elsewhere in this Journal otherwise you will lose out on the significant benefits of membership. These include:

- free attendance at our late afternoon meetings
- free quarterly journal
- 20% reduction in the subscription price of the *Computer Fraud and Security Bulletin*
- 20% reduction in the subscription price of *Computers and Security*
- a saving of at least £75 on our own Annual Conference
- 25% reduction in the subscription to the *Quality Software Report* newsletter
- discounts on attendances at many other conferences and training opportunities
- the opportunity to take part in our twice yearly Discussion Group

As Corporate membership costs only £75, you will realise that membership of the Group can actually save your organisation many hundreds of pounds each year.

☛ RENEW NOW TO RETAIN THESE IMPORTANT BENEFITS ☚

Contact our Membership Secretary, John Bevan, on 01992 582439 if you would like further information.

BOOK REVIEW

TITLE: **Opportunity Makes a Thief (An Analysis of Computer Abuse)**

AUTHOR: Audit Commission

PUBLISHER: HMSO

ISBN: 0-11-886137-9

PRICE: £8.50

PAGES: 40

Another three years have come and gone since the last survey by the Audit Commission and once again their sober analysis of the state of control, or rather the lack of it, in British computer systems lands on my desk. The two authors, Chris Hurford and Diane Skinner, will be well known to many of you by their trademark of a total lack of sensationalism in their reporting. Here are the facts, devoid of the more usual embellishments that one associates with the reporting of computer abuse. It is this very soberness that makes this triennial survey such chilling reading. It is not the figures themselves that cause the chill, although a 183% increase in reported incidents would make any other organisation shout it from the rooftops, it is the simple fact that computer abuse occurs because of a lack of basic controls rather than sophisticated manipulation. This is no different from the Commissions findings of ten years ago.

The Commission sent out 5,500 questionnaires and received 1,073 replies. A twenty percent response rate is not bad, but as usual, it leaves that feeling of unease that things are actually worse than the findings indicate. That, however is neither the point, nor the lesson from this authoritative survey. It is simply the fact that the implementation of quite basic controls would have prevented, or at least detected, the abuses much earlier than was the case. I am not going to reproduce the figures for you here. You really should go and purchase a copy, no a number of copies for your organisation. Make it a present for your chief executive, the members of the audit committee and the director of I.T. It is not a long read, but it is a worthwhile one. Especially the 'computer abuse assessment' checklist at the rear. It may be teaching grandmother to suck eggs, but I am sure that the chairman of your audit committee would prefer to learn how to do that rather than end up with egg on his face.

John Mitchell

Guidelines for Potential Authors

The Journal publishes two types of article: refereed and invited. Refereed articles should be technically oriented, and based on current or future issues related to computer audit, security or control. This type of article will be reviewed by at least one member of the editorial panel (anonymously). If published, it will be identified as a refereed paper.

An invited article need not be technical or overly academic (even Computer Auditors have a sense of humour!). In fact it need not even be 'invited'. Submission without invitation is encouraged and although this may lead to severe sub-editing by the Editor, submission will virtually guarantee publication.

We also invite members to volunteer for book, product and course reviews (anonymously if required).

Why not call Rob Melville at CUBS (0171 477 8646) to discuss how you can get your name in print?

Management Committee

CHAIRMAN	John Mitchell	LHS - The Audit & Control Consultancy	01707 654040
SECRETARY	Raghu Iyer	KPMG Peat Marwick McLintock	0171 236 8000
TREASURER	Nigel Smith	NJ Associates	01707 334421
MEMBERSHIP SECRETARY	John Bevan	Audit and Computer Security Services	01992 582439
JOURNAL EDITOR	Rob Melville	City University Business School	0171 477 8646 SC355@CITY.AC.UK
MEMBERS MEETING	Paul Howitt	Tesco Stores Limited	01992 632222 Ext 2320
	Jenny Broadbent	Cambridgeshire County Council	01223 317256
DISCUSSION GROUPS	Bill Barton	The Rank Organisation PLC	01883 623355
	Steve Pooley	Independent Consultant	01580 891036
	Alison Webb	Independent Consultant	01223 461316
	Jim Ewers	Hertford County Council	01992 555328

Membership Enquiries to:
John Bevan
46 Queens Road, Hertford,
Herts SG13 8AZ

01992 582439

casg
Computer Audit Specialist Group

The British Computer Society

PLEASE RETURN TO
John Bevan
Membership Secretary

46 Queens Road
Hertford
Herts SG13 8AZ

Membership Application/Renewal

(Renewals are due in August of each year)

I wish to APPLY FOR / RENEW (delete as appropriate) my membership of the Group in the following category and enclose the appropriate subscription.

CORPORATE MEMBERSHIP (Up to 5 delegates)* £75
* Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal and attendance at our meetings (see over)

INDIVIDUAL MEMBERSHIP (NOT a member of the BCS) £25

INDIVIDUAL MEMBERSHIP (A member of the BCS) £15
BCS membership number: _____

STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment). Educational Establishment: _____ £10

Please circle the appropriate subscription amount and complete the details below.

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: (Please circle) 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)
SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS CASG"
AND RETURN WITH THIS FORM TO THE ADDRESS SHOWN ABOVE

ADDITIONAL CORPORATE MEMBERS

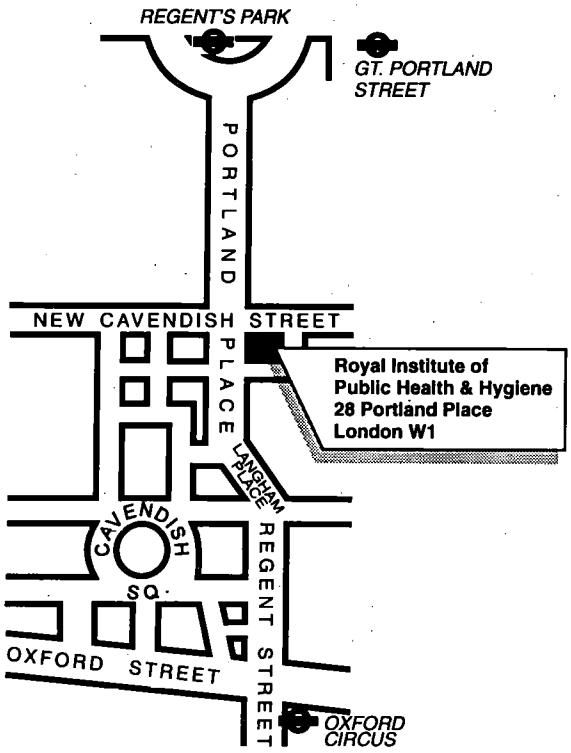
INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify

Venue for Members' Meetings



SUBMISSION DEADLINES

Spring Edition	**14th February**
Summer Edition	**14th May**
Autumn Edition	**14th August**
Winter Edition	**14th November**