ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 8 NUMBER 1 AUTUMN 1997

The British Computer Society

Technical Briefings 1997/98

For more details of all Technical Briefings, and details of costs and registration, contact Jean Brown, on 01803 872775

IT and the Law
15 October 1997 at the Royal Aeronautical Society, London
Chairman: Willie List, BCS Security Committee

The Procurement Process	Rosemary Boyle, Cambridgeshire County Council
What goes wrong	Hilary Pearson, Bird and Bird
What to put into the contract	Alan Laing, Oracle
Shrink-wrap licensing - Data protection implications	Christopher Millard, Clifford Chance
Expert Witness in IT	Ron McQuaker, President, British Computer Society

---

Electronic messaging
27 January 1998 at Chartered Accountants' Hall, Moorgate Place, London
Chairman: Steve Hinde

Connectivity and the accountant	Malcolm Marshall, KPMG
open.gov: the electronic delivery of government services	Matthew Bishop, Cabinet Office
Uses and abuses of e-mail	Daniel Strawson, Electric Mail
Electronic Lodgement	Brian Handley, Project Officer, Electronic Lodgement, Inland Revenue
Commerce and the Internet: Auditing Implications	Freddy MacMarne, NatWest Electronic Markets

---

Looking beyond the Millennium
28 April 1998, at the Royal Aeronautical Society, London
Chairman: Martin Robinson, IIA

Auditing a RAD Project	Jennifer Stapleton, Vice-President of the BCS, and Chair of the Technical Board
Major Projects: what can go wrong	Brian Helbrough, Imago
Using the benefits of hindsight - the role of post-project analysis	Arnold Kransdorff, Pencorp Ltd
Penetration testing	John Austen, BA FBCS, Computer Crime Consultants
Fraud investigation and internal security	Tom Mulhall, BT

Followed by the Annual General Meeting.

Contents of the Journal

CASG Technical Briefings 1997/98		Front Cover
Editorial	John Mitchell	3
Chairman's Corner	Alison Webb	4
The Competencies of the Excellent Information Systems Auditor - Refereed Article	Sarah Blackburn	5
BS7799 - Draft Consultation Paper		14
Change Control in the PC LAN Environment- The Effect of Murphy's Law	Bob Ashton	17
Science Now?		18
BCS Matters	Colin Thompson	19
	Hazel Roberts	20
CASG Matters - Report from the Cash Box	Bill Barton	21
Membership Committee		22
Management Application		23

Submission Deadlines

Spring Edition	7th February
Summer Edition	7th May
Autumn Edition	7th August
Winter Edition	7th November

The ***Journal*** is the official publication of the Computer Audit Specialist Group of the British Computer Society. It is published quarterly and is free to members.

Letters to the editor are welcome as are any other contributions. Please contact the appropriate person on the editorial panel.

Editorial address:
47 Grangewood,
Potters Bar
Herts, EN6 1SL

Designed and set by Carliam Artwork, Potters Bar, Herts
Printed in Great Britain by Post Script, Tring, Herts.

EDITORIAL

Well the summer has come and gone, together with England's chance of regaining the Ashes (much to the glee of my Australian Friends), and we are at the beginning of a new season for the Group and the eighth year of *The Journal*. This edition contains the Treasurer's report for the year, which shows that we remain on a firm financial footing, despite the fact that, after advertising income, *The Journal* cost £5,000 for the year. This was however, a thirty percent reduction on the previous year. How did we achieve this saving?

Three main ways. First, we reduced the print size, so that we now get more words on less pages. This may mean that you all need to go out and purchase 3x reading glasses, but think of the benefit to the Group's reserves! Second, we now get almost all our material in electronic format, which helps to keep our type setting costs down. Third, we have increased our advertising revenue. Two things that we have not done is to decrease the quality of the content, or the number of issues.

This edition contains our usual mix of news and articles. We have an article from Bob Ashton, a previous Committee member who now works in Australia, on the trials and tribulations of performing a network upgrade. You will also find another of those 'howlers' from across the pond, this time on science matters. Martin Welsford has responded to David Chadwick's plea for help on the teaching of spreadsheet control and Hazel Roberts, our very own BCS librarian, has provided some Internet/Intranet titles which will be of interest to many of you.

We also have Colin Thompson's column on our parent body and a refereed article from Sarah Blackburn on what is needed to be a good IS Auditor. Sarah has concluded that paper qualifications are not enough and I well remember her comment during a presentation in Wellington, New Zealand (name dropper) earlier this year. Sarah said, 'I may well be a CISA qualified auditor, but I still can't audit a Unix system'. Read her article and decide for yourself, whether or not, you really are qualified to do your job!

John Mitchell

Chairman's Corner

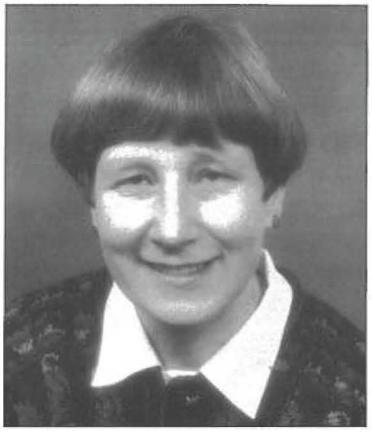
Alison Webb

I was talking to a Head of Audit recently who said that when assessing the effectiveness of systems in controlling risks, he looked first at the management control structure and at the information systems managers used. Second in his hierarchy of evidence was analytical review. The testing he did was minimal: it was too expensive, he thought, for the amount of evidence collected.

I was thinking this over and wondering why it made me vaguely uneasy yesterday, when summer-pruning my fruit trees. (You may be reading this in October, but I'm writing it in July: John Mitchell believes in deadlines.) I'm not an expert gardener, and when I planned to fan-train a cherry tree against my garden wall, all I knew about pruning was that I'd have to do some. I bought an excellent paper-back gardening book, which set out the theory extremely well, explaining the why as well as the what, and I set out with the book in one hand and my secateurs in the other. But I found, as everyone does, that the tree at the bottom of the garden hadn't read my text-book: it hadn't formed new laterals and fruiting buds where it was supposed to. I was stuck. I called in a couple of friends as consultants: they gave me conflicting advice. In the end, I gingerly made a few tentative cuts, and retired to the house to watch the tree die.

Actually, it didn't: and ten years on, the tree is beautifully-behaved and very fruitful. Yet nothing has changed: I haven't bought any more gardening books, or asked anyone else how to prune, nor do I call in a tree surgeon each summer. Simply, I've had ten years of trying to do what it said in the book without ruining the tree, and now I really understand how the practice may modify the theory.

I looked at an access control system the other day where I thought that the controls that ensured all users were authorised were impeccable. Any user wanting access sent a suitably authorised form to the system administrator, who, with his two assistants, were the only people with sufficient



privilege to change the user base. The administrator had Personnel reports regularly of leavers, so he could remove them from the system, and he scanned monthly reports of those who hadn't accessed the system for six months. I won't go on: theoretically it was fine.

But when I scanned a list of userids, I found that of the total of 4,000, over 500 had a person associated with them described in the security database only as "UNKNOWN". There was a rush job on, involving a lot of contract staff, so the administrator had set up a batch of 500 extra ids, and allowed a user to assign them as she needed by passing on the passwords. So much for the forms and the controls. This is the problem with control structures as with gardening books: users, like trees, are far more complex and interesting than our text-book descriptions of them.

Audit testing doesn't just show up instances where people aren't following the rules: it highlights areas where something has happened the rules don't cover and that we may not have thought about. More rules aren't necessarily the answer: we all know that complicated instructions, whether about operating a video recorder or running a business process, take an age to write, tend to obscure the principles that really matter and are rarely read anyway.

So Art will ever exactly mirror Life, as far as management control structures are concerned. While this is the case, I'll remain a fan of testing.

The Competencies of the Excellent Information Systems Auditor

Sarah Blackburn

ABSTRACT

Recruiting and retaining competent information systems auditors has never been harder. As organisations expect greater added value from their auditors a wider range of professional skills and interpersonal behaviours is needed. How can we identify and develop talent to meet this need? This paper explores the two main models of competency world-wide, one based on standards of performance, the other on underlying behaviours, showing how each of them could be applied to real information systems audit environments. It challenges whether paper qualifications are enough to certificate the senior information systems auditor, to differentiate the information systems auditor from other professionals or to guarantee satisfactory performance.

INTRODUCTION

How should we define a competent information systems auditor? Is it competence when an individual consistently performs work to the standards required over a range of contexts or conditions? (Finn, 1993) Or is competence an underlying characteristic of a person which is causally related to effective or superior performance? (Hooghiemstra, 1992) Solon said: "Call no man happy till he dies." (Herodotus, 1996) This suggests that happiness must be constantly reinforced in action. Should we say the same for competence? Or once competent will someone always be so?

There are at least three interested parties to the competence debate surrounding information systems auditors: the employers, professional bodies and not least the individual auditors themselves.

The employers of information systems auditors want to recruit staff of a given level of competence at a price so that with or without further training and development they will carry out competent pieces of information systems audit work in that firm. Hence they are interested in the predictive value of competence indicators: if I hire someone with BCS, QiCA or CISA qualifications, will this person perform better audits with less supervision?

Of its nature information systems auditing is a young profession compared to accountancy or general audit. Information systems auditors may be members of the British Computer Society (BCS), the Institute of Internal Auditors (IIA), the Information Systems Audit and Control Association (ISACA) and/or an accountancy body: or they may have membership of none of these but be qualified by experience. Eraut (1994) states that professions exist to provide social control of expertise. "Experts are needed to provide services which the recipients are not adequately knowledgeable to evaluate" and thus to protect them from incompetence, carelessness and exploitation. (Eraut, 1994) ISACA, for example, would provide such protection through its professional Body of Knowledge (the five domains of its CISA syllabus), its General Standards on Information Systems Auditing and its Code of Professional Conduct (ISACA, 1997).

Eraut (1994) describes the characteristics of a profession as:

"the underpinning knowledge and understanding of concepts, theories, facts and procedures;
the personal skills and qualities required for a professional approach to the conduct of one's work;
the cognitive processes which constitute professional thinking."

This goes much farther than passing examinations and assessments or even possessing the personal skills and qualities which many employers test for using commercially available occupational personality tests. It implies a particular way of thinking and approaching situations which call for professional judgement. Schon (1983) describes this as a process of reflection in which the professional applies knowledge and experience to each unique situation.

Individual information systems auditors need to assert their employability. Membership of a professional body and the acquisition of its qualification are a waste of effort unless the value of that membership and qualification are recognised and valued by employers.

Thus all three parties are looking for a clear differentiation between information systems auditors who can do the job and others. What makes that difference? Is it a division between qualified and experienced information systems auditors on the one hand and people less well qualified and experienced on the other or are there other factors?

This paper describes the two main movements in competency thinking and links them to information systems professionals. Following the majority of writers on this subject, the term *competence* is used generally to denote overall ability in performance. *Competencies* are underlying characteristics of a person which are causally related to effective or superior performance? (Hooghiemstra, 1992) *Competences* are examples of work to prescribed standards over a given range of contexts or conditions (Finn, 1993).

THE COMPETENCY MOVEMENT

A traditional view of competence (Finn, 1993) is contained in any job description which sets out the main tasks involved in the job and the list of qualifications and years of experience need to fulfil the role. Both can be misleading in terms of defining the right person to do the job well (Cabanis, 1996).

There are two main schools of thought in the competence field, the Standards and the Behavioural. Their ideas about competence spring on the one hand from looking at what skills are required to do a particular job, and on the other at what a skilled person can do. This difference of focus between the job and the person is fundamental. The differences are summarised in Table 1.

Table 1: Comparison of behavioural and standards models of competence/competency

Behavioural model : "Competencies"	Standards model : "Competences"
Focused on the individual, the superior performer in the role	Focused on the job and on the minimum competence levels
Aims to predict competent behaviour	Sets criteria for recognition or accreditation of competent performance
Competencies can be motives, traits, self- concepts, attitudes or values, content knowledge or cognitive or behavioural skills. hand and personal characteristics on the other	Competences are standards of performance which are recognised by some writers to draw on knowledge and understanding on the one
Mainly US and UK	Mainly UK, Europe, Australia, New Zealand, some US bodies
Favoured by companies	Favoured by governments and professional and trade associations

The Behavioural School

Although Adams (1996) considers the origins of the competency based education and training theories may go back to the 1920s, the US behavioural competency movement started in the 1950s with a Harvard psychologist, David McClelland (Spencer et al 1994). McClelland (1973) identified principles for doing research to identify competency variables which did predict job performance and which were not biased (or at least, less biased) by race, sex or socio-economic factors (Spencer et al 1994). He adopted the use of criterion samples: comparing people clearly successful in their jobs with persons less successful in order to identify operant thoughts and behaviours causally related with success (Spencer et al 1994). McClelland had previously worked on motivation (McClelland, 1961, McClelland and Winter, 1969, McClelland and Burnham, 1970) and he adapted methods used there to his study of competency (Spencer et al, 1994): the Behavioural Event Interview technique combining elements from Flanagan's critical incident method (Flanagan, 1954), the Thematic Apperception Test (McClelland, 1961) and scoring of transcripts by Content Analysis of Verbal Expression (CAVE) (Zullow et al., 1988).

In particular McClelland (McClelland and Dailey, 1973) showed that traditional academic examinations did not predict job performance or success in life and were often biased against minorities, women and poorer people. For example, he looked at US diplomats and found that neither the General Aptitude Test Battery nor the General Background Knowledge Test scores predicted future success on the job but that the differentiating characteristics of the better diplomats were cross-cultural interpersonal sensitivity and maintenance of positive expectations of others despite provocation, coupled with speed in learning political networks. (Spencer et al, 1994)

Richard Boyatzis (1982) developed McClelland's ideas further and defined effective performance as the attainment of specific results (outcomes) through specific actions while maintaining the policies, procedures and conditions of the organisational environment. He also distinguished between threshold competencies and superior competencies. Threshold competencies are those essential to performing a job in a minimally adequate way but which do not lead to superior performance: for example, speaking the native language of subordinates; using the software standard in the organisation. Superior competencies mark out the high flyers (Finn, 1993).

Knowledge, skills, self-concepts (attitudes or values), motives and traits are all considered competencies in the behavioural model (Spencer et al 1994). Knowledge by itself appears rarely to distinguish superior from average performer and is thus classified as a threshold competency (Finn, 1993). Skills can be both cognitive and behavioural (Spencer et al 1994). Self-concepts relate to what people value, how they see themselves and what they are interested in (Spencer et al 1994). Motives are the underlying need or thought patterns which drive, direct and select an individual's behaviour (Spencer et al 1994). McClelland (1987) identified the need for Achievement, the need for Power and the need for Affiliation as the three most important motives. A trait is a general disposition to behave or respond in a certain way, such as self-confidence, self-control and resilience under stress (Kobasa et al, 1982).

Figure 1 shows a representation of the relationship between knowledge, skills, self- concepts, motives and traits. Motives and traits are most deeply embedded in personality: knowledge and skills are the behaviours that can be changed most easily _ but only if the person is sufficiently motivated (Spencer and Spencer, 1993). Recruitment, however, is often centred on knowledge and skills, although underlying values, attitudes, traits and motives may be of greater significance in distinguishing the superior performers (Spencer et al 1994).

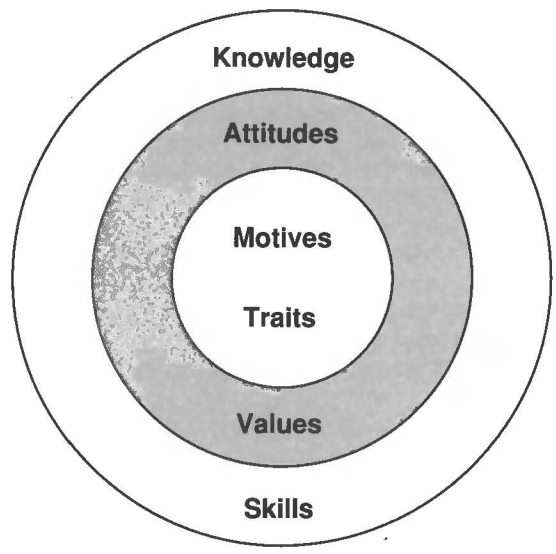


Figure 1: The Onion Skin Model
(after Spencer and Spencer, 1993)

Boyatzis (1982) identified six main clusters of behavioural competencies for managers in general as shown in Figure 2.. There is some disagreement as to whether management competencies are universal across all organisations or specific to each organisation. Spencer and Spencer (1993) catalogued differences by functional

specialism while Dulewicz and Herbert (1992), Finn (1993) and Matthewman (1995) found similarities between company specific lists. Dulewicz (1990) writes "I have often given a "guestimate" that 70% are general requirements across different organisations and 30% are organisation specific." Schroder and Cockerill (1990), aiming to integrate theories of managerial competence and cognitive style, found high performance management competencies universally applicable but more likely to be relevant to a dynamic and rapidly changing organisation. However, Smith et al (1989) found differences in skill requirements did exist between sectors for those employing recent business and law graduates. Whitley (1989) also concluded that "Ownership of skills is more organisational and less individual."

Later writers (Spencer and Spencer, 1993) have explored the behavioural competencies of a variety of occupational groups. Much work has also been carried out within organisations (for example, Dulewicz, 1990) but the present writer is unaware of published work on information systems auditors.

The Standards School

The work of McClelland has been largely ignored by the publicly-funded competence movement in the United Kingdom (Adams, 1996) where the occupational standards programme of the Department for Education and Employment and the work of the National Council for Vocational Qualifications (NCVQ) are predominant. This approach stemmed from a historical concern with establishing *minimum* competence standards for certification and licensing (Eraut, 1994). The focus is on job-oriented functional analysis which has been used to break down the roles and tasks of an occupation to small elements (Finn, 1993). Then each element of competence is matched up to performance criteria to indicate the minimum level of competence. The resulting analysis shows all the activities or outcomes a job-holder will demonstrate in that job. Levels of National Vocational Qualifications (NVQs) have also been set (from 1 to 5) which are claimed to demonstrate standards from technical and clerical to managerial levels across professions and occupational groups. In Australia as well at least twenty professions are developing competence standards in response to a government initiative (Stretton, 1995). Following the classification adopted by Gonczi et al (1990), a profession needs to define the knowledge, skills and attitudes of its practitioners and to have set standards as the criteria for measuring their performance (outcome competencies). One of the features of outcome competencies, and perhaps a secret of their attractiveness to government, is that they can form the basis of an assessment and hence a qualification. It may be debated whether such qualifications differ greatly from traditional qualifications (Stewart and Hamlin, 1992).

Where the Standards model may fall short is in explaining the underlying knowledge, skills and attributes which the competent performer brings to his/her role in order to achieve those outcomes (Stewart and Hamlin, 1992, Crawley, 1995). What works to the

Figure 2: Summary of Management Competencies (after Boyatzis, 1982)

Cluster	Motive	Trait	Self-concept	Skill
Goal and action management	concern with impact			concern with impact
			diagnostic use of concepts	diagnostic use of concepts
	efficiency orientation		efficiency orientation	efficiency orientation
			proactivity	proactivity
Leadership				conceptualisation
			self confidence	self confidence
			use of oral presentations	use of oral presentations
			logical thought*	logical thought*
Human Resource management				managing group processes
			use of socialised power	use of socialised power
Human Resource management (cont'd)				accurate self assessment*
			positive regard*	
Directing subordinates			developing others*	developing others*
				spontaneity*
			use of unilateral power*	use of unilateral power*
Focus on others				perceptual objectivity
		self control		
		stamina and adaptibility		
Specialist knowledge			Specialist knowledge*	

* Threshold competencies

satisfaction of the NCVQ in manual occupations has failed to satisfy those describing the competence of newly qualified management accountants in the UK, for example (Matthews, 1992).

The Management Charter Initiative (MCI) in the UK has attempted to bridge the gap between standards and behavioural competencies. Although the occupational standards are in line with the official approach, the MCI has also developed a personal competency model to identify the behavioural competencies that distinguish superior performers. The MCI standards stress that performance of the competence elements is underwritten by knowledge and understanding on the one hand and by personal characteristics on the other (Henley Management College, 1993).

Figure 3 suggests a relationship between the two main competence models based on ideas put forward by Robinson (1996). Although the arrows flow forwards from the deep seated motives to the visible outcomes, in practice one needs to work backwards from what can be seen and measured. Skills and values may be either innate or learned and the two may feed off each other. Neither will come to anything without the impetus of motivation. As discussed above the role of experience is questionable. It is shown here as a filter through which innate and learned abilities act to produce outcomes. Although some degree of experience is necessary, those with the relevant innate abilities or previously learned abilities may require less to achieve successful outcomes. Knowledge and understanding support and underlie the movement from the potential of the abilities to the actual outcomes.

Since this representation is not linear, an alternative model for more practical purposes is offered in figure 4 as used for an Institute of Chartered Accountants in England and Wales Board for Chartered Accountants in Business working party (1997). Here the relationships are tabulated. The fourth column, labelled Competence and Outcomes, lists the activities of the internal auditor at a summary level. They could be further analysed into individual elements although experience has shown that it is difficult if not impossible to assign knowledge, skills and attributes to low level elements without much duplication and confusion.

Application to Information Systems Auditors

Examples of the Standards approach to auditor competencies are relatively common. The UK Chartered Institute of Management Accountants has created elements for internal audit work although they have not been formally published (Matthews, 1992). The UK Institute of Internal Auditors (1997) has also looked at standards for internal auditors. The US Institute of Internal Auditors (1997) has a research project in progress with a target completion date of First Quarter, 1998. This is the Competency Framework for Internal Auditing (CFIA). This research adds to the profession of internal auditing _

> *by identifying the current state of internal auditing practices as a basis for 1) updating The Common Body of Knowledge for Internal Auditing; and 2) providing a "snapshot" of the practice of internal auditing on a global basis. The CFIA will also provide documented evidence to determine programs and forums, continuous educational developments, and the content, structure, and format of future research and training programs in internal auditing. Accordingly, the study will identify international practice issues and trends in internal auditing and provide information about the work activities performed by internal auditors and the Competency Framework needed by practising internal auditing practitioners.*
>
> (IIA,1997)

The US Department Of Energy (1997) has prepared a department-wide Functional Area Qualification Standard for Defence Nuclear Facilities Technical Personnel which includes descriptions of outcomes which are information security related and which are each listed with supporting knowledge and/or skills. However, the emphasis appears to be on knowledge and theory rather than skills and actions. For example:

> *"2.22 Safeguards and security personnel shall demonstrate a familiarity level of knowledge of the classified computer security program as described in Department of Energy (DOE) Order 5639.6A, Classified Automated Information System Security Program, and DOE Manual 5639-6A.1, Manual of Security Requirements for the Classified Automated Information System Security Program.*
>
> *Supporting Knowledge and/or Skills*
>
> *a. Describe the types of automated information system security activities that are classified.*
>
> *b. Discuss examples of classified automated information system security programs.*
>
> *c. Identify and describe the classified automated information system security standards, policies, procedures, and objectives related to safeguards and security."*

Figure 3. An Integrated Competency Model

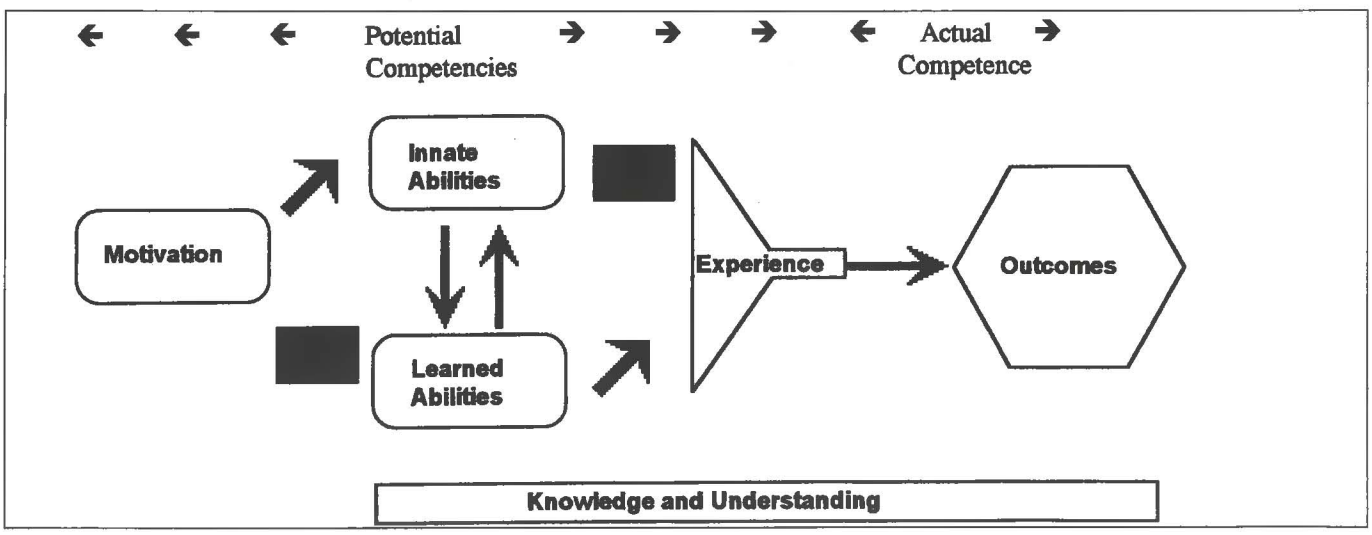


Figure 4: Description of Internal Auditor Competencies for the Board of Chartered Accountants in Business, 1997

1997: The Scenario
Reporting usually to a finance director, Internal Audit covers a wide range of activities from financially oriented compliance work, through physical audits to support accuracy of accounts (mainly stock audit), to operational review of any area throughout the business. Internal auditors conduct independent audits of existing processes. In many instances they also audit new systems whilst under development and have begun to facilitate control self assessment. Since 1990 the size of departments has decreased but there are more departments than previously (in response to Cadbury) and the level of qualified staff is greater. Although risk is a key component in the direction of audit effort, elements of risk are managed independently in a number of other financial and non financial areas such as Treasury and Insurance. The majority of internal auditors are qualified as accountants, internal auditors and computer audit professionals.

Competencies			**Competence**
Knowledge	**Skills**	**Attributes**	**Outcomes**
• General and specific knowledge of strategic management issues • General understanding of systems and processes and types of control • Specific knowledge of systems and processes in own company and its industry • Awareness of legal and regulatory requirements (financial and non financial) • Understanding of risk identification and quantification techniques • Knowledge of systems development methodologies and practices • Knowledge of project management techniques	• Interviewing for information Recording of processes • Evaluation of risks and controls • Computer assisted audit techniques for obtaining evidence • Analytical review techniques • Report writing • Oral presentation • Use of PC as personal productivity tool • Facilitation with individuals and groups	• Open to new information and experiences • Speed of learning about new areas • Empathy with client balanced by perceptual objectivity • Insatiable curiosity • Persistence • Ability to work with detail balanced by ability to see the whole • Diagnostic use of concepts • Efficiency orientation	• Identifies audit universe and prioritises audit effort on risk basis • Maintains awareness of internal and external risks throughout organisation • Plans and controls audit projects • Obtains audit evidence • Reports findings to client management and to Audit Committee • Facilitates client understanding of risk and control • Persuades the need for change where indicated by mismatch between risks and controls

The example in figure 5 is taken from the Internal Audit department of a UK retail organisation and has been put into the format used by the example in figure 4.

This example was one of several related competency specifications for different roles used by that audit department and demonstrates another important aspect of competency: range or scope (Finn, 1993). The information systems auditor described here conducted interviews for information and audit clearance, but not for recruitment or appraisal purposes as more senior members of the department did. He or she influenced auditors and client staff up to senior management level but did not have to work with directors.

The example also brings together both outcomes and behavioural competencies. The attributes were the last part of the framework to be added and there was some controversy as to whether they represented learned behaviours or innate attributes. Since the framework was to be used in appraisals there was some feeling that innate attributes should not be included as the basis for rewards.

Qualifications and experience criteria were included from the departmental job descriptions. In practice less well qualified and experienced people were often recruited as information systems auditors and then trained and qualified on the job. In effect, therefore, personal attributes were being used in recruitment, albeit unsystematically.

The writer has recently carried out some preliminary research into the skills and attributes of internal auditors although this did not distinguish between information systems and non information systems auditors. Using the technique created by McClelland and Boyatzis (Spencer et al 1994) a small sample of successful internal auditors (information systems and general) was interviewed and asked to recount critical incidents they had been involved in on audits in the last eighteen months. Some of the most common behaviours which were reported are shown in figure 6 together with verbatim examples.

I have not found any published work on the personal qualities of information systems auditors. It is an opportunity for an individual to research and for a professional body to fund. I have carried out some very limited investigations of auditor (including information systems auditor) competencies from which only tentative conclusions may be drawn as to the competencies of information systems auditors.

The Certified Information Systems Auditor (CISA) qualification of the Information Systems Audit and Control Association (1997)

Figure 5: Description of Internal Information Systems Auditor Competencies for a UK retail organisation.

Information Systems Auditor
Role: Works on a succession of similar audit projects using prescribed departmental techniques. Minimum experience: 8 years computing and audit experience including work with IBM mainframe, PC networks, Systems Development Life Cycle, Project Management. Qualifications: BCS, CISA, MIIA/QiCA

Competencies			Competence
Knowledge	**Skills**	**Attributes**	**Outcomes**
• All departmental methodologies for audits and reviews. • General and specific knowledge and understanding of management issues throughout the company where they relate to information systems • General understanding of systems and processes and types of control • Specific knowledge of systems and processes in this company and its industry • Understanding of risk identification and quantification techniques • Knowledge of systems development methodologies and practices • Knowledge of project management techniques	• Time management and project scheduling techniques • Interviewing for information • Conduct of meetings for negotiation • Evaluation of risks and controls • Analytical review techniques • Report writing • Use of PC as personal productivity tool • Mainframe interrogation skills using departmental software • Downloading and preparing data for other auditors to review using CAATs. • Oral presentation • Use of body language positively in communication	• Willing to listen • Willing to learn • Empathises with client • Displays commitment to quality in work. • Presents arguments rationally • Uses facts to support arguments • Ensures facts are accurate numerically and in words • Appreciates needs of others in team • Sense of urgency to finish • Completes work honestly • Good attendance, punctual	• Plans own work on projects. • Conducts interviews for information and for audit clearance. • Conducts meetings with staff from clerical level up to middle and senior management • Evaluates controls in technical systems and related non-technical systems. • Writes standard and non standard correspondence and report drafts on technical subjects in plain language. • Conducts analysis applying a range of techniques including computer assisted. • Co-ordinates tasks in liaison with non information systems auditors. • Leads and coaches less experienced auditors • Builds working relationships in audit teams • Trains and develops less experienced auditors including non information systems auditors • Makes presentations to other departments including information systems professionals • Influences other auditors, and client staff up to senior management level.

Figure 6: Most Common Internal Auditor behaviours in a UK retail organisation.

Behaviour	Relative frequency	Examples
Curiosity and questioning for information	1	"Every time she talked about relationships with senior management in Merchandise I asked her more about that because I'm quite interested in that. Merchandise is a bit of an unknown quantity to me. And because I don't know anything about that I want to. Because it's there." "I was trying to ask fundamental planning questions as regards what his function was, what areas he would like us to look at in the audit but his agenda was quite different, I think, trying to find out who had written the [previous] audit report which he thought was totally factually incorrect."
Develops others	2	*Anomaly caused by the sample, all of whom had had significant exposure to secondee auditors in the previous year.* "I sat down with D and between us we produced the planning document, now I made him type most of that, I sat him at my terminal and made him type as we discussed the work I made him sit there because D had no background on PCs at all, so it was quite a new thing for D to sit down and use a PC and type things in."
Seeks hard evidence and supports arguments with facts	3	"I left it at that point that I would read the contract and meet with him again and as I left his office I took him with me to his secretary so that he could instruct her to give me a copy and I waited and got the copy there and then and took it back to my desk." "I think in the end I spent another 3 days digging round invoices, rechecking, rechecking the signatures, rechecking the paperwork, but on the positive side I found a raft more of errors which I recognised during the first lot of work but had not felt they were significant enough to include in the main findings."
Establishes relationships	=4	"I made some general comments about his lizard on his desk. There were a few moments of chit chat before we started the meeting proper to discuss the findings in the audit report."
Sees potential for loss	=4	"I became aware that the system development people were about to enter into a contract which was worth about £2 million that had not gone through the legal dept or the purchasing dept and was with one company with whom I was suspicious about their relationship."
Persuades client of concerns	6	"I think what clinched it was when I described to B that (almost casting Distribution as the baddies) that Distribution was cancelling special orders and that was causing his people grief because the systems were out of line so the stores were continually sending in special orders that Distribution were cancelling resulting in several days delay before the store found out, told the customer, irate customers lost sales and that it was costing B's people in the stores aggravation . . . and when I described it like that he immediately said `Well, we need more communications to sort this out, we cannot have these people causing my people problems."
Seeks assurance of audit members	7	"I discussed it with my colleagues who shared my concerns and individually and collectively we made representations to the head of audit."
Plans audit work	8	"I had previously prepared a list of questions which I had to ask basically about the processes through which I was hoping to determine whether they had organised processes or not and I also had arranged for a visit to the offices and to the physical warehouse location to actually be walked round and have a look at the operations."
Understands complex scenarios	9	"And the other half they'd actually brought in professional project managers and neither set got on with the other and neither set seemed to be doing any better than the other. So all the projects in my opinion were in trouble. They were getting budget squeezes on them so they were chopping functionality all over the place but they were not integrated with each other sufficiently and I could foresee horrendous problems because they'd got 3 or 4 projects that were all radically changing the same system" "The meeting with the merchandise manager was quite significant. Not so much from the facts gained but from the impressions gained from the meeting that it was a contentious area."

provides via its five job domains is a list of outcomes from which the knowledge input is relatively easily derived but skilled behaviours and attributes are not. Figure 7 illustrates the problem. Is it the knowledge that makes a CISA a competent information systems auditor to whom you would entrust an audit? Or is that just a threshold competency? Is what makes the difference the other skills and attributes?

CONCLUSIONS

This paper contends that what internal audit departments should recruit for in information systems auditors is not just knowledge or even experience. There is a need to identify the attitudes and skills and deeper qualities of people who are more capable. Given a choice between a candidate with the right skills and attitudes or a more knowledge candidate without those qualities it is taking a bigger risk to appoint the latter than the former. It is easier to improve the level of knowledge and train in relevant skills than to change innate or habitual behaviours. ■

Figure 7: CISA Job Domains (ISACA, 1997)

Domain	Outcome	Knowledge of:	Implied skills/attributes
Domain 1 - Information Systems Audit Standards and Practices and Information Systems Security and Control Practices (8%)	Adheres to generally accepted information systems audit standards, statements and practices, and information systems security and control practices.	Information systems audit standards, statements and practices, and information systems security and control practices.	Respect for professional values and ethics.
Domain 2 - Information Systems Organisation and Management (15%)	Analyses and evaluates the information systems (IS) strategy, policies and procedures, management practices, and organisation structures.	Information Systems strategy. Best practice policies, procedures and practices.	Analysis techniques. Audit planning. Audit reporting. Other???
Domain 3 - Information Systems Process (22%)	Analyses and evaluates the information systems (IS) process, including hardware and software platforms, network and telecommunications infrastructure, operational practices, utilisation of information systems resources, and business processes.	A range of hardware and software platforms. Networks and telecommunications systems. Operational best practice. Human resources scheduling. Business specific processes.	Analysis techniques etc.
Domain 4 - Information Systems Integrity, Confidentiality, and Availability (29%)	Analyses and evaluates logical, physical, environmental, data validation; processing and balancing controls; and the business continuity planning and testing process.	Controls over integrity, confidentiality, and availability.	Analysis techniques etc.
Domain 5 - Information Systems Development, Acquisition, and Maintenance (26%)	Analyses and evaluates information systems (IS) development, acquisition, and maintenance.	Systems Development Life Cycle. Project management. Procurement.	Analysis techniques etc.

REFERENCES

ADAMS K (1996), 'Competency's American Origins and the conflicting approaches in use today', *Competency*, 3, 2, pp 44 - 48

BOARD FOR CHARTERED ACCOUNTANTS IN BUSINESS (1997), *Response to Institute of Chartered Accountants in England and Wales paper on Accountancy in 2005*, in publication.

BOYATZIS R E (1982), *The Competent Manager: A Model for Effective Performance*, John Wiley and Sons

CABANIS J (1996) 'Your Career: The Project of a Lifetime', *PM Network*, April, pp 20 - 24

CRAWLEY R (1995) 'The future of the MCI Management Standards', *Executive Development*, Vol 8, No 6, pp 35 - 39

DULEWICZ V (1990) 'Assessment Centres as the Route to Competence', *Personnel Management*, November.

DULEWICZ V & HERBERT P (1992) *Personality, Competences, Leadership Style and Managerial Effectiveness*, Henley Working Paper 14/92

ERAUT M (1994), *Developing Professional Knowledge and Competence*, The Falmer Press, London

FINN R. (1993) 'A Synthesis of Current Research on Management Competencies' Henley Management College Working Paper 10/93

FLANAGAN JC (1954) 'The Critical Incident Technique', *Psychological Bulletin*, Vol 51, No 4, pp 327 - 358

HOOGHIEMSTRA T (1992) 'Integrated Management of Human Resources', *Competency Based Human Resource Management*, Mitrani A, Dalziel M and Fitt D (Eds), Kogan Page London

HERODOTUS (1996) *Histories* I.32, Selincourt A D (Tr); Marincola J M (Ed) Penguin, London

GONCZI A, HAGER P, OLIVER L (1990), *Establishing Competency-Based Standards in the Professions*, National Office of Overseas Skills Recognition, Research Paper No 1, Australian Government Publishing Service, Canberra

HENLEY MANAGEMENT COLLEGE (1993), *The Development of Senior Management Standards: Final Report*

KOBASA SC, MADDI SR, KAHN S (1982), 'Hardiness and Health: A prospective study', *Journal of Personality and Social Psychology*, 42, pp 168 - 177.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA) (1997) World Wide Web: http://www.isaca.org

INSTITUTE OF CHARTERED ACCOUNTANTS IN ENGLAND AND WALES (1997), *Response to 2005 Paper*, to be published.

INSTITUTE OF INTERNAL AUDITORS (US) (1997), World Wide Web: http: // www. Rutgers .edu / Accounting / raw/iia/

MATTHEWMAN J (1995) 'Trends and Developments in the use of Competency Frameworks' *Competency*, Vol 2 No 4 Supplement

MATTHEWS S (1992) 'Occupational Standards in Management Accountancy', *Management Accounting*, May pp 48 - 50

McCLELLAND D C, (1961) *The Achieving Society*, Princeton NJ, Van Nostrand

McCLELLAND D C, (1973) 'Testing for competence rather than intelligence' *The American Psychologist*, , Vol 28 No 1, pp 1 - 40

McCLELLAND DC (1987), *Human Motivation*, Cambridge, Cambridge University Press.

McCLELLAND DC, DAILEY C (1973), *Evaluating new methods of measuring the qualities needed in superior foreign service information officers*. Boston, McBer and Company

McCLELLAND D C, BURNHAM D H, (1976) "Power is the Great Motivator", in Vroom V H, Deci E L, 1970, 1992, *Management and Motivation*, Penguin, London, pp 231 - 240

McCLELLAND D C, WINTER D G, (1969) *Motivating Economic Achievement*, The Free Press, New York

ROBINSON A (1996) *Presentation on Competence*, Henley Management College

SCHON DA ((1983, reprinted 1996), *The Reflective Practitioner*, Arena, Aldershot

SCHRODER HM, COCKERILL AP (1990) *Managerial Competence and Cognitive Style: its implications for the management of creative scientific work*, Centre for Organisational Research Working Paper Series No 002, London Business School

SMITH D, WOLSTENCROFT T, SOUTHERN J (1989) 'Personal Transferable Skills and the Demands on Graduates', *Journal of European Industrial Training*, Vol 13, pp 25 - 31

SPENCER LM, McCLELLAND DC, SPENCER SM (1994), *Competency Assessment Methods. History and State of the Art*, Hay McBer ResearchPress

SPENCER LM, SPENCER SM (1993), *Competence at Work: Models for Superior Performance*, John Wiley

STEWART J, HAMLIN B (1992) 'Competence-based Qualifications: The Case against Change,' *Journal of European Industrial Training*, Vol 16, No 7, pp 21 - 32

STRETTON A (1995) 'Australian Competency Standards', *International Journal of Project Management*, Vol 13, No 2, pp 119-123

US DEPARTMENT OF ENERGY (May 1995), 'Safeguards And Security Qualification Standard Competencies' World Wide Web: http://cted.inel.gov/cted/qualstd/saf-sec.html

WHITLEY R (1989) 'On the Nature of Managerial Task and Skills: Their Distinguishing Characteristics and Organisation', *Journal of Management Studies*, Vol 26, No 3

ZULLOW HM, OETTINGEN G, PETERSON C, SELIGMAN MEP, (1988) 'Pessimistic Explanatory Style in the Historical Record', *American Psychologist*, Vol 43, No 9, pp 673 - 682

Sarah Blackburn,
Henley Management College, United Kingdom

Sarah Blackburn is the Head of Group Internal Audit at Kingfisher plc. Her undergraduate degree was from Cambridge University. After some years spent teaching and lecturing, she qualified as a Chartered Accountant with KPMG. She worked for five years in internal audit for J Sainsbury plc, where she was responsible for information systems audits, achieved her CISA and completed her MBA at Henley Management College. For four years she was Head of Group Internal Audit for Argos plc. She is now a part-time doctoral associate of Henley Management College where she is researching the behavioural competencies of project managers.

BS7799

The Group is taking an active part in the revision of the BSI Security Standard. The following should provide you with a flavour of the consultation process - Ed.

Draft Consultation Paper on The Future Revision of BS7799

V5.0 (19th May 1997)

1. INTRODUCTION

This consultation paper sets out some proposals and ideas for a possible future revision of BS7799. These proposals stem from the UK BSI/DISC Business Development Group Committee BDD/2, which at its meeting on the 16th January, addressed the question of a revised version of BS7799. The BBD/2 discussion concentrated on the scope and general nature of a revised standard, the level of detail and areas to be included, supporting documents, and the need for international collaboration.

General Nature of the Revised Standard

It is proposed that the revised standard should be broad enough to accommodate all issues concerning the management of information security within an organisation. It should not address detailed technical aspects, many of which are, in any case, the responsibility of international groups within ISO, IEC, JTC1 and liaison organisations. Where there was a need to refer to them, it should do so and cross refer to other supportive material. As such, it is proposed that the revised standard should retain a high level prescriptive style and be supported by a series of other documentation wherever possible. This would obviate the need to make constant changes to the standard.

International Collaboration

It is proposed that work on a future revision of BS7799 should involve the international community to make it more suitable for international use. Any consultation and revisions to BS7799 should therefore be done in consultation with the international community, especially those countries which have already adopted BS7799 as a standard (e.g. The Netherlands, Australia and New Zealand) and those countries that are considering doing so. It should be noted that there is already feedback from some countries who wish to be involved in such a collaborative effort.

Consultation Document

This consultation document has been prepared by BDD/2 and outlines ideas for a proposed way forward. It will be used in consultation with industry, commerce and user groups and other interested parties, to obtain comments and ideas on a revised version, and to decide how to move any revision work forward.

2. PROPOSED DOCUMENT ARCHITECTURE

In keeping with the discussion presented above, it is proposed that a two tier document architecture, as illustrated in the figure below, should be adopted as the basis for a revised standard.

Top Layer

At the top layer BS7799 (Part 1) and the BS7799 Specification (Part 2) would be positioned. At this layer BS7799 would concentrate on high level management principles. The structure of Part 1 would remain the same as it is in the currently published version of BS 7799: topic areas, control objectives and controls. Part 2 is a specification, currently being developed in the UK, to support UK accreditation. Part 2 contains Part 1 control objective statements written in a way that they can be used as part of an accreditation scheme i.e. they can be used as 'conformance statements' in the traditional sense of ISO 9000 and similar standards.

It is not intended to make changes to the structure or radical changes to the content of Part 1. The structure, as indicated above should remain the same, the only difference being that additional material may need to be added where necessary, e.g. additional controls. Also the level of detail describing the controls shall be made more consistent throughout Part 1. More detailed guidance information would be provided by supporting documents at the lower layer.

Lower Layer

At the lower layer various documents could be referenced that support the implementation of the control objectives in BS7799 Part 1. These documents will provide the more detailed guidance necessary to assist in the implementation of the management of information security.

It is envisaged that there would be a set of documents each concentrating on a specific topic. For example, the UK DTI have produced, with industry and government, documents related to 'Protecting Business Information' which could be positioned at this layer, for UK users of the standard, in support of the high level requirement for classification labelling (Clause 3.2.2 in the current version of BS7799).

Other examples include various international and national standards and guidelines that have been published such as the PIN management standards from TC68, NIST and other sources (which would support Clause 7.3.1) or standards on physical security from IEC and BSI (which would support Clause 5).

Types of Supporting Document

Documents at the lower level could include commercial standards and implementation guides, trade association documents, national and international standards and guidelines and other guidance material already in existence (see examples below). Where specific guidance does not exist in whatever form then it may be necessary to develop such documentation

3. EXAMPLES

The following examples illustrate the possible mapping between the high level principles within BS7799 and what could appear as lower level supporting documents.

BS7799 Section/Clause	• Example Supporting Document(s)
1.1 Information Security Policy	• ISO/IEC 13555-3[2] GMITS Part 3 Techniques for the Management of IT Security • AS/NZS 4360 Risk Management
3.2 Information Classification	• UK/DTI publication (Protecting Business Information)
5 Physical and Environmental Security	• BS7083
7.3.1 Password Use	• FIPS 112 (Password Usage) (US/NIST publication) • ISO 9564 PIN Management
7.4 Network Access Control	• Firewall guidelines contained in ISO/IEC 13555-5 GMITS Part 5 • German Baseline Protection Manual
All sections	• Systems Auditability and Control Report, Institute of Internal Auditors Research Foundation (UK) • OECD publication OCDE/GD(92) 190 Guidelines for the Security of Information Systems

[2] Department of Trade and Industry. The scope of this international Technical Report covers providing guidance and advice on different approaches and methods for risk assessment, and including establishing a baseline approach.

4. OPEN ISSUES, COMMENTS AND QUESTIONS

The issues and questions presented below have been identified as some of those that need to be addressed when considering a revision of BS7799, however there may be other issues that are identified in the course of the consultation process.

Answers and contributions are welcomed on these and other issues that might be identified in the course of the consultation process.

4.1 Consultative Questions

Scope

> Should the scope of the standard be 'Information Security' or should it be limited to just IT security?

A general opinion is that the title (Information Security Management) should remain and the scope of the document should be aiming at this title and not be limited to just IT. In which case there is a need to broaden the current scope and content.

Target Audience

> Who should the target audience be? For example, is it sufficient to address the person responsible for implementing information security within an organisation or is there a wider audience?

Level of Detail

> What is an appropriate level of detail? Is the current level of detail just right, too much, or too little?

The level of detail in the current version of BS 7799 is not consistent. For example, in some places there is a lot of detail e.g. on password controls and on other topics there is very little detail e.g. in the area of compliance. The revised standard should be consistent in the level and depth of detail. Based on comments received the exact level of detail will be determined during the drafting of the revised version.

Document Architecture

> Should the two-tier document architecture given in clause 2 of this document be adopted?

It is suggested that the revised standard needs to be structured to ensure that it can cope with the fast moving world of technology, i.e. no area should be so proscriptively defined as to make it unworkable should the technology change. In keeping with clause 2 a revised 7799 standard should cover the high level management principles, and refer to lower level standards for supporting guidance, and more detailed specific controls.

Areas of Coverage

> Are there any areas, control objectives or controls that are not covered by the current standard? If there are new things to be covered, please identify these and suggest how should they be dealt with in a revised version of the standard?

4.2 Other Issues and Comments

Definitions and Terminology

There is a need to ensure that any definitions given in the standard are used consistently throughout the document and that they are appropriate to its scope. For example, in the case of confidentiality, integrity and availability, these terms are defined different-

ly elsewhere. The actual definitions to be adopted will be selected during the preparation of the revised version. Supporting Documents There may be different types of supporting document e.g. related to specific national aspects, specific sector issues, or specific topics, or one devoted solely to relevant international standards. The range, scope and availability of supporting documents needs to be agreed. It is intended to establish a mechanism to reference a supporting documents e.g. using an Internet Web site.

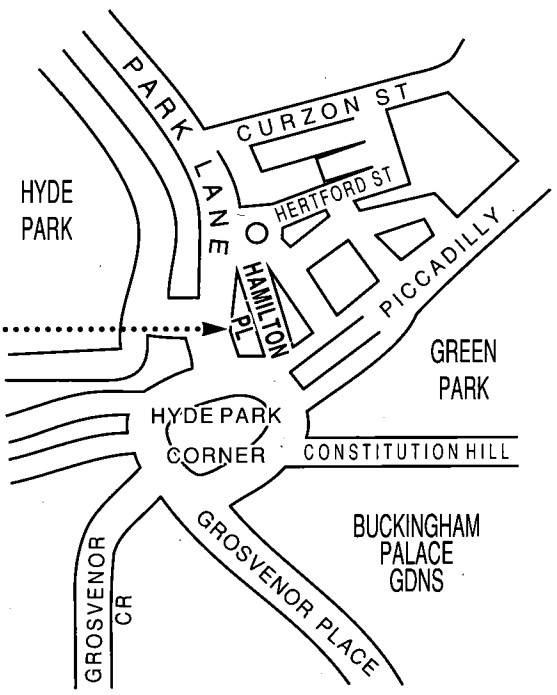
5. PROPOSED TIMETABLE

The following is a proposed timetable to take forward the revision process.

Activity	Time	Comments
Public consultation	May - Sept 97	Parallel activity in each of the countries involved
Workshop in the UK	Nov 97	Joint workshop
Agree BS7799 revisions	Nov 97	Joint meeting
Drafting period for revised 7799	Nov 97- Feb 98	UK lead activity with international participation from countries involved
Review of revised version	Feb 98	Parallel activity in each of the countries involved
Public comment period	Feb - June 98	Parallel activity in each of the countries involved
Editing period	July 98	Joint editing meeting
Publish revised version	end of 98	Parallel activity in each of the countries involved

Venue for Technical Briefings

Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ



Change Control in the PC LAN Environment - The Effect of Murphy's Law

Bob Ashton

This is a real life story taken from company with which I am familiar, and illustrates the kind of problems which can occur when sound change control procedures are not in place.

The purpose of a change control system is to minimise the risk of failure of a production system or application. There is an inherent risk of introducing an error associated with implementing any change. A change control system is a methodology of updating application and system changes in a controlled, systematic way to ensure that only authorised changes are implemented.

The company in question runs a number of Novell Netware LANs. The LAN Manager needed to upgrade the memory of one of his servers. He had already performed this operation on a number of occasions, and each time it had been a simple job. You just take the case off, unplug one lot of SIMMs (single inline memory modules) and plug in the new ones.

It was now 7 o'clock in the evening, and as usual, many users, including the accountants and senior managers, were still logged on, having ignored an earlier broadcast warning message. This had been sent at 4:30 to all LAN users explaining that the service would not be available after 7:00 pm, and requested them to log out before that time. The LAN Manager therefore had to forcibly log these users out.

The old SIMMs were removed and the new ones inserted. Unfortunately, the Vendor had supplied him with SIMMs which were not the correct speed for the machine (70 ns instead of 60 ns). The Manager thought he had finished his work for the night when he rebooted the server and was looking forward to some well earned rest, when he found that he had problems with error messages regarding the speed of the chips. His problems increased when he replaced the original SIMMs and rebooted, as he found that all data on the RAID (redundant array of inexpensive disks) was now lost. Curious readers will no doubt be wondering how changing the volatile memory could possibly affect data on the hard drives. To save time the LAN Manager had added new disks to the RAID box at the same time as he was making this minor change to the server, and had configured the extra disks while the server was in configuration mode for the changed SIMMs. When the server was rebooted the new disks had been configured as part of the array. The LAN Manager then tried to return the system to its original state by removing these disks, taking with them indexing and data. The combined effect of these changes resulted in the data on the RAID becoming inaccessible. At this point he concluded that the system was irrecoverable.

Although it was now getting very late, the LAN Manager was not too concerned as he thought he had taken all necessary precautions. After all, the fileserver was equipped with the ARCserve backup/restore utility, and he had a shelf full of DAT tapes which were automatically written every night at midnight. Using this system he was able to rebuild the entire system, starting with disk partitioning, installation of the Novell operating system, reinstalling all the applications and finally restoring both the last weekly full backup and the last daily incremental backup.

It was now well into the early hours of the next day and the LAN Manager congratulated himself on the use he had been able to make of his skills and knowledge of the system recovering from such a serious situation, and went home to bed satisfied that a good job had been done. However, the LAN Manager's problems were now escalating fast as it was the time that the Accountants did their month end spreadsheet work. They had spent the last 3 days on this but had not saved their data once, and the version of ARCserve then in use was not able to save open files. They complained bitterly when they were told that they would have to do it all again. Also, when users are forcibly logged off a Novell LAN, open files on their PCs are at risk. As a result, data owned by some of the senior managers who had ignored the request to log out was lost. This group also complained bitterly.

The LAN Manager's background was in PCs. In the PC world people have always been contemptuous of the glacial pace of change in the mainframe world, and this was one of the principal drivers in the early success of the PC. If you want to make a change to your PC you go ahead and do it on the fly. If you got it wrong you just try again. Change control procedures in the mainframe world are characterised by a disciplined approach, have a safe backout strategy at all stages, are bureaucratic in nature, and take a long time.

It was not the fault of the LAN Manager that the accountants had been foolish enough not to have saved their spreadsheets, or that senior managers had chosen to ignore his good advice, and surely he was doing his best to get through two of his many tasks as quickly as possible. The LAN Manager was fired.

An older, and possibly wiser Manager was asked advice on sound change control procedures for the LAN and these have now been implemented. Carefully thought backout plans are now produced for all changes before anything is done. These detail how changes can be reversed out, if necessary, so that the system can be re-instated to the status which existed before the change. This is particularly important where a testing platform is not available, which is generally the case with LANs.

Change plans are now fully documented in advance, and discussed and signed off by all involved before anything is done. Just like 30 years ago.

The change control process now consists of the following steps:

- Reason for the change - documented.
- What is going to be changed - documented.
- A dry run detailing the steps to be taken is documented. This is to prevent the system administrators from making changes on the fly.
- The risk of failure is assessed, and steps needed to reverse changes if things go wrong are documented.
- All stakeholders of the system are notified. This is done by email, with receipt confirmation.
- The document containing all these steps is then authorised by the IS Manager, and signed off by the user.
- Changes are done over the weekend.

A memo has been issued to all LAN users stressing the importance of logging out when asked to do so, and of saving their work frequently. This is reissued quarterly. The ARCserve program has been upgraded to a later release which can save open files.

Murphy's Law states that anything which can go wrong will go wrong, and this seems to have happened here. Some people think that you are not a real driver until after you've had your first accident, and no doubt this particular LAN Manager is both a lot more cautious and meticulous in his approach in his new employment. The moral of this story is that technology management have to be aware that when anything serious goes wrong with their systems, it is they who are ultimately held responsible. It is the duty of auditors to remind them of this simple fact of life. ■

Some members may recall Bob Ashton who was a Committee member for a few years up until 1988. At that stage he decided to move to New Zealand where he spent a year with the Government and 5 years in the Banking Industry. Bob is CISA qualified and arranged the CISA revision course for the Wellington Chapter. Wishing to live in a warmer climate, Bob moved to the Sunshine State of Queensland and spent 2 years working in the Wagering Industry, which, as anyone who has visited Australia will know, is very popular in that part of the world. Over the past year Bob has managed the IS Audit function in a major mining and manufacturing group. Bob can be contacted on ara@qld.mim.com.au

Science Now?

The beguiling ideas about science quoted below were gleaned from essays, exams, and classroom discussions in the USA. Most were from 5th and 6th graders. They illustrate Mark Twain's contention that the 'most interesting information comes from children, for they tell all they know and then stop.' - Ed.

We say the cause of perfume disappearing is evaporation. Evaporation gets blamed for a lot of things people forget to put the top on.

The law of gravity says no jumping up without coming back down.

When they broke open molecules, they found they were only stuffed with atoms, But when they broke open atoms, they found them stuffed with explosions.

When people run around and around in circles we say they are crazy. When planets do it we say they are orbiting.

Some people can tell what time it is by looking at the sun. But I have never been able to make out the numbers.

Clouds just keep circling the earth around and around. And around. There is not much else to do.

Thunder is a rich source of loudness.

Isotherms and isobars are even more important than their names sound.

One horsepower is the amount of energy it takes to drag a horse 500 feet in one second.

You can listen to thunder after lightning and tell how close you came to getting hit. If you don't hear it you got hit, so never mind.

Talc is found on rocks and on babies.

Rainbows are just to look at, not to really understand.

While the earth seems to be knowingly keeping its distance from the sun, it is really only centrificating.

Someday we may discover how to make magnets that can point in any direction.

South America has cold summers and hot winters, but somehow they still manage.

Most books now say our sun is a star. But it still knows how to change back into a sun in the daytime.

Water freezes at 32 degrees and boils at 212 degrees. There are 180 degrees between freezing and boiling because there are 180 degrees between north and south.

A vibration is a motion that can't make up its mind which way it wants to go.

There are 26 vitamins in all, but some of the letters are yet to be discovered. Finding them all means living forever.

There is a tremendous weight pushing down on the center of the Earth because of so much population stomping around up there these days.

Lime is a green-tasting rock.

Many dead animals in the past changed to fossils while others preferred to be oil.

Genetics explain why you look like your father and if you don't why you should.

Vacuums are nothings. We only mention them to let them know we know they're there.

Some oxygen molecules help fires burn while others help make water, so sometimes it's brother against brother.

To most people solutions mean finding the answers. But to chemists solutions are things that are still all mixed up.

In looking at a drop of water under a microscope, we find there are twice as many H's as O's.

Clouds are high flying fogs.

I am not sure how clouds get formed. But the clouds know how to do it, and that is the important thing.

Water vapor gets together in a cloud. When it is big enough to be called a drop, it does.

Humidity is the experience of looking for air and finding water.

We keep track of the humidity in the air so we won't drown when we breathe.

Rain is often known as soft water, oppositely known as hail.

Rain is saved up in cloud banks.

In some rocks you can find the fossil footprints of fishes.

Cyanide is so poisonous that one drop of it on a dogs tongue will kill the strongest man.

A blizzard is when it snows sideways.

A hurricane is a breeze of a bigly size.

A monsoon is a French gentleman.

It is so hot in some places that the people there have to live in other places.

The wind is like the air, only pushier.

BCS MATTERS

Colin Thompson
BCS Marketing Director

A new BCS Medal

Recognising achievement is an important function for any professional body and the BCS is to introduce a new medal, to be presented to individuals who have made a major contribution to the advancement of Information Systems.

The medal is to named the Lovelace medal, after Ada Lady Lovelace, daughter of the poet Lord Byron, who was educated as a mathematician and scientist. In collaboration with Charles Babbage she developed descriptions of both the Difference Engine and the Analytic Engine and it is through her work that the real genius of Babbage has been recognised. Ada Lovelace was the first woman to be intimately involved in Computer Science, long before it was formally recognised as a discipline, and in 1979 a software language, developed by the US Department of Defence was named in her honour.

The Lovelace Medal will be awarded for the first time during the Society's 40th anniversary year which commences in October 1997. Nominations should be forwarded to Andy Lewis, the BCS Registrar, by 31 January 1998.

New BCS Publications

The publications area has been particularly active over the past year, due in part to the success of the report of the Year 2000 Working Party under the title The Year 2000 a practical guide for professionals and business managers. That success looks set to continue with the publication of the second volume of that report. Volume 2, published in August contains 64 pages and takes a more in depth look at the problems associated with the millenium date change. As part of this, the report covers 6 key areas - Personal Computers, microprocessors and controllers, tools, testing, human resources and legal issues. An A1 size year 2000 wallchart accompanies the report.

Also published in August was a report entitled "preparing for the EURO". The IS related problems associated with Economic and Monetary Union have received less attention than the year 2000 issue up to now. But they are no less real or urgent, and many systems will need substantial modification, whether or not the UK adopts the single currency. The new BCS publication, which has a foreword by Howard Davies, is intended to raise the awareness of both the business and the professional communities.

Still with publications, the new BCS Review and Directory will be available in mid October. As in previous years the review will contain a range of articles on current issues within the IS field together with information on the BCS itself. The Directory element of the publication will be carried this year on a CD Rom containing a listing of all BCS Professional members plus an extensive range of other information, including an electronic version of the Review plus volume 1 of the Year 2000 report.

The above mentioned publications are available from the Customer Service Department at BCS HQ (Tel. 01793 417 424 or e-mail marketing@bcs.org.uk) priced as follows:

TITLE	MEMBER	NON MEMBER
Year 2000 Volume 1	£7.5	£10
Year 2000 Volume 2	£15	£20
Review and Directory	£10 Pre publication £15 Post publication	£65
Preparing for the EURO	£15	-

Finally, before leaving the subject of publications, news of changes to the Computer Bulletin. This will include a new editorial team, led by John Kavenagh, a freelance journalist who has produced the BCS page in Computer Weekly for some years. As from October the magazine will have a new design and a range of new features with a more journalistic approach, which we hope will provide members with a more lively and interesting read.

The proposed BCS Security Register

Work on the new Register of Information Security Practitioners is now nearing completion. We expect to see the Security Register open for business in October and it is the intention that it should become the prime source of information for anyone seeking reliable, professional advice and guidance on security matters. Registrants must be professional or Companion members of the Society must also meet requirements in respect of both information systems engineering and security experience. Sponsorship will be required and all applicants will be interviewed by Assessors.

Anyone interested in receiving further information in respect of the new register should complete the slip attached to the leaflet enclosed with this newsletter, or contact the Customer Service Department at BCS HQ.

.....and the proposed Computer Consultancy Register

Regular readers of this column may recall that the Society is also considering the introduction of a Consultancy Register. Subject to Council approval, this is planned for introduction in 2 stages: stage 1 will cover the first 2 to 3 years of operation and will involve listing on the basis of information submitted by the registrant; stage 2 will introduce a validation regime similar to the Security Register. As with the Security Register, BCS membership is mandatory.

Further information in respect of the Consultancy Register is also available from Customer Services.

Dispute Resolution Services

A recently published leaflet sets out brief details of the BCS services in the area of dispute resolution. These services include the nomination of members with established skills as arbitrators or expert witnesses or to provide expert determination or mediation. Copies of the new leaflet are available from Customer Services.

And Finally.....BCS Annual Dinner

AGM and Annual Dinner time approaches yet again and this year's dinner, scheduled for 17th October, is set to be a very special event. To mark the fact that the dinner is the opening event of the Society's 40th year, the dinner is to be held at the Guildhall in association with the Worshipful Company of Information Technologists. The Guest speaker will be Lord Baker and musical entertainment will

be provided by the band of the Royal Corps of Signals.

Subject to the normal formalities of the AGM, which takes place earlier in the day, this will be the first event in the presidential year of Sir Brian Jenkins. For further details - and tickets - contact Karen Sullivan at Headquarters (01793 417 434).

Requests for further information on these, or any other BCS related issues, should be addressed to Colin at The British Computer Society, 1 Sanford St Swindon SN1 1HJ or by e-mail to cthompson@bcs.org.uk

Letter to the Editor

Spreadsheet Troubles

I am writing in response to David Chadwick's article on spreadsheet control and his request for help (Volume 7, No. 4).

I have one example of errors using spreadsheets. This is where the spreadsheet is used simply to aid the presentation of a reconciliation. In my example, the person concerned typed several items and values and then totalled them using a calculator - in other words she did not use the sum capability of the spreadsheet. As a result she made a calculation error and the totals were incorrect.

The risk is that her manager assumed that the spreadsheet calculated the sums and that therefore the reconciliation was accurate, when it wasn't. If the manager had spotted the total error, there might have been much time wasting searching for an incorrect entry because of the assumption that the spreadsheet cannon make a mistake adding up. Also, had an important decision been based on the result of the reconciliation, (it wasn't, thank Goodness), then the wrong decision would have been made.

The advice that Daniel gave in the article about the three A's, is good and I will remember that and apply it when the opportunity arises. But I feel that a spreadsheet is like any other application of IS and should be specified and documented. It should also be checked before being used in a live situation. The person doing the checking, (testing), should be aware of the context and objective of the spreadsheet application, hence the need for reasonable documentation and specification. No need to go over the top but a brief narrative, perhaps as part of an introduction to the work sheet, is advisable.

I hope this helps. -

Martin Welsford BA QiCA

Tel (Work): +44(0)1705 834203
Tel (Home): +44(0)1983 562137
E-mail: martin@welsford.softnet.co.uk

Library Update

Hazel Roberts - BCS Librarian

Since my last column, the IEE/BCS Library has recently acquired a number of publications on Internet/intranet security which are listed below. If you are interested in looking at any of these publications or want to find out about any other subjects then you are welcome to visit the Library or contact us by e-mail, telephone or fax. Our contact details are at the end of this column. The Library is open from 9.00am until 5.00pm, Monday to Friday. If you are not a member of the BCS or the IEE then you are still welcome to use our Library facilities for reference purposes. Only IEE or BCS members are eligible to borrow books.

If you would like to search the Library catalogue without having to spend time travelling down to visit the IEE building in London, then our catalogue can be found on the Institution Of Electrical Engineers' Internet home page.

The URL for the Library page is: http://www.iee.org.uk/Library/. From there you will be able to find the catalogue. After searching the catalogue and finding a particular book of interest, it is possible for members to order this item on loan by completing a "borrowers" form which is emailed to the Library desk. A librarian will check the details and send you a reply. If available, the book will be sent to you by registered post and should arrive within 3-4 working days.

Further details about the Library and our services can be found on the Library home page.

INTERNET SECURITY 1997

1-56604-506-1
PAGAN K , FULLER S
Intranet firewalls: planning and implementing your network security system.
Ventana, 1997

1-85032-301-X KYAS O Internet security: risk analysis, strategies and firewalls
International Thomson, 1997

0-12-455835-6
LOSHIN P
TCP/IP clearly explained
Academic, 1997

0-07-882240-8
SHELDON T
Windows NT security handbook Osbourne
McGraw-Hill, 1997

0-12-045597-8
AHUJA V
Secure commerce on the internet
Academic, 1997

0-07-021389-5
FEIT S
TCP/IP: architecture, protocols and implementation with IPv6 and IP security.
McGraw-Hill, 1997

Hazel can be contacted at:

The IEE/BCS Library,
The Institution of Electrical Engineers,
Savoy Place,
London, WC2R 0BL.
Telephone: 0171 344 5461.
Facsimile: 0171 497 3557.
E-mail: hroberts@iee.org.uk or
E-mail: libdesk@iee.org.uk
World Wide Web: http://www.iee.org.uk/

REPORT FROM THE CASH BOX

Bill Barton - Treasurer

The Group had a very successful year financially. There was a surplus of £4,731 for the year compared with a deficit of £3,259 for the prior year.

The most significant factor was an increase in income from the Technical Briefing Sessions of 58%, due primarily to the increase in prices from £40 plus VAT to £65 plus VAT. These sessions still provide excellent value for money. Also there was a reduction in the costs of printing and distributing the journal which fell by 27%.

We also increased our income from advertising in the journal by £600.

With a slight increase in charges for the technical briefing sessions next year we anticipate there will be another surplus next year.

THE BRITISH COMPUTER SOCIETY - COMPUTER AUDIT SPECIALIST GROUP

INCOME AND EXPENDITURE ACCOUNT FOR THE YEAR ENDED 30 APRIL 1997

	1996/97	1995/96
Income	£	£
Technical Briefing Sessions and other meetings	13,942	8,802
Subscriptions	6,294	6,285
Interest on Bank Accounts	1,099	1,218
Journal Advertising	750	150
Other Income	165	0
	22,250	16,455
Expenditure		
Technical Briefings Sessions and Other Meetings	10,886	9,610
Journal	5,758	7,896
Printing, postage and other administrative expenses	875	1,607
Prior Year Items	0	601
	17,519	19,714
Surplus/ (Deficit) for the Year	£4,731	-£3,259
Fund Balance	£	
Fund Balance at 1 May 1996	26,882	
Add 1996/ 97 surplus	4,731	
Fund Balance	£31,613	

There's no fool like . . . .

A friend of mine works at a large insurance company as a system administrator. He informed his boss that the boss's hard disk needed to be "balanced."

My friend gave his boss a program which writes "weight files" on carefully computed spots on the disk, so that the balanced disk will run smoother. The boss distributed the program among the employees and ordered them to regularly have their hard disks balanced!

casg
Computer Audit Specialist Group

British Computer Society

Management Committee

CHAIRMAN	Alison Webb	Consultant	01223 461316 amwebbcam@aol.com
SECRETARY	Raghu Iyer	KPMG	0171 311 6023 raghu.iyer@kpmg.co.uk
TREASURER	Bill Barton	BSkyB	0171 766 1685 bartona@sky.bskyb.com
MEMBERSHIP SECRETARY	Jean Brown		01803 872775 100125.66@compuserve.com
JOURNAL EDITOR	John Mitchell	LHS - The Business Control Consultancy	01707 851454 lhs001@aol.com
SECURITY COMMITTEE LIAISON	John Bevan	Audit & Computer Security Services	01992 582439
TECHNICAL BOARD LIAISON	Geoff Wilson	Consultant	01962 733049
	Allan Brown	Consultant	01803 872775 alan.brown@aduk.co.uk
TECHNICAL BRIEFINGS	Diane Skinner	District Audit	0117 9001418 dskinner@district-audit.gov.uk
	Jim Jackson	Lombard North Central plc	01737 774111 jjackson@lombard.co.uk
	Paul Plane	National Westminster Bank plc	0171 726 1882
	Tom Harper	First National Bank of Chicago	0171 580 8350 tharper@fnbc.com
	Jenny Broadbent	Cambridgeshire County Council	01223 317256 jenny.broadbent@finance.cambscnty.gov.uk
	Mike Demetriou	Lombard North Central	01737 744111 mdemetriou@lombard.co.uk

Membership Enquiries to:

Jean Brown
26 Rosehill Gardens
Kingkerswell
Newton Abbot
Devon
TQ12 5DN

British
Computer
Society

PLEASE RETURN TO
Jean Brown
CASG Membership Secretary
26 Rosehill Gardens
Kingkerswell
Newton Abbot
Devon
TQ12 5DN

Membership Application

(Membership runs from July to the following June each year)

I wish to APPLY FOR membership of the Group in the following category and enclose the appropriate subscription.

CORPORATE MEMBERSHIP (Up to 5 members)* £75

* Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal *(see over)*

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

INDIVIDUAL MEMBERSHIP *(A members 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)