IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

JOURNAL

volume 13 number 1-2 spring 2003 ISSN 0961-9348

Programme for members' meetings 2002/2003 season

Tuesday 1st October	**DATABASE SECURITY**	Evening 16.00 for 16.30 to 18.00 KPMG
Monday 4th November	**IMPLEMENTING AND AUDITING IT GOVERNANCE**	Full Day Briefing 10.00 to 16.00 Chartered Accountants' Hall Moorgate Place London EC1
Tuesday 3rd December	**BS7799**	Evening 16.00 for 16.30 to 18.00, KPMG
Tuesday 28th January	**CYBERCRIME UNCOVERED**	Full Day Briefing 10.00 to 16.00 Central London
Tuesday 11th February	**DIGITAL SIGNATURES**	Evening 16.00 for 16.30 to 18.00, KPMG
Tuesday 18th March	**SYSTEMS DEVELOPMENT & AUDITING**	Full Day Briefing 10.00 to 16.00 Central London
Tuesday 13th May	**HACKERS** *Presenter: John Butters - The Ernst & Young Tiger Team* *An inside view of an attack and penetration squad that uses skills that go beyond normal penetration testing. As well as off-site attacks, they use techniques to gain access into computer networks which include physical entry via ceilings, stolen key cards and social engineering.*	Evening 16.00 for 16.30 to 18.00 KPMG

To be preceded by IRMA AGM

Please note that these are provisional details and are subject to change.

The late afternoon meetings are free of charge to members.
For full day briefings a modest, very competitive charge is made to cover both lunch and a full printed delegate's pack.
For venue maps see inside back cover.

Contents of the Journal

The ***Journal*** is the official publication of the Information Risk Management & 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
Email: john@lhscontrol.com

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

Editorial

One of the few bonuses of doing this job is that I get the occasional opportunity to rant about some of the stupid things that I find when going about my everyday business. Now one of the reasons I became an auditor was because I liked the apparent power without responsibility advantage that it conferred upon me. I soon learnt that this was not the true situation, but it did give me access to senior people who would give me the courtesy of a hearing, even if they did not subsequently do anything about the problem I had identified.

Editorship gives a similar illusion of power without responsibility, but again one has to take one's responsibility seriously, so before ranting off I always give the other party the opportunity to respond to whatever I am going to write. In this case the cause of my rant was (notice the past tense) the Standard Life Assurance Company. A few months ago I registered for their on-line service so that I could track the depreciation in my pension policy. They require, amongst other data, my national insurance number. I enter it in the very format that is printed on the pension document provided to me by Standard Life 'AA NN NN NN', but it is rejected. I try again with the same result. I then guess that it should be AANNNNNN and it is accepted. Hooray! Spoke too soon. The next box to pop up states that this is my registration number and I should write it down as it is the only future way to access my details. There is no method of saving the details to my computer, so I am forced to write it down on an insecure piece of paper. The number is 10 digits long! I am then asked to select a pin number. This is only 4 digits long and as I can choose my own I do not need to write it down. I am then offered the opportunity to tailor my own site. Yes please. However, first I must register again!

Okay, in for a penny and off I go, but this registration is different. The identifier is my email address and I can choose any password that I like. This is good, because I can use my normal mix of alpha numerics and can make it longer than 4 digits. So, we have the same company with apparently two different sites designed by different people. The really important one, the one with my pension details requires me to write down a 10 digit number, but only requires a 4 digit password. The second site uses my email address, which is in the public domain, but allows me to choose a strong password. Crazy. I try to find someone to discuss these matters with. Tricky. I can talk to all sorts of people about products, they are listed on the site, but nowhere is there any direct link to a webmaster, or technical support.

I try a thing called a user guide and find a number for technical problems. Now I have a design problem, not a technical problem, but no-one else seems to fit the bill so I call technical support (not a free number) and talk to a chap whose name I will withhold. He points out very firmly, bordering on the insulting, that my problem is not technical. I agree with him and he suggests that as I have registered a pension I should speak to the pensions help desk. He kindly puts me through, or rather I get stirring music for 10 minutes.

I then talk to another person who is polite and explains that the first 6 digits of the pension registration number are my date of birth, therefore I only need to remember the last 4. Goodness, this is worse than I thought. Loads of people know my date of birth, so Standard Life's security over its customer data depends on a 4 digit identifier and a 4 digit password. Nought out of ten for security. I can see that their security people have never heard of CISSP. I insist on a written response. He asks whether an acknowledgement of my concern is sufficient. I respond that I want a detailed answer to my points. He wriggles, but eventually agrees to email me something.

A few days later I received the following response which I print in full because it is a fine example of excellent customer relations. 'I am responding to the comments made to one of my colleagues regarding the frustrations you encountered registering for services on our website today.

Firstly, we appreciate all customer feedback and really do listen to what customers have to say which in some cases can help us identify new improvements, or, as in the case of online registration, can help ratify the changes we are already making.

The views expressed in the Journal are not necessarily shared by IRMA. Articles are published without responsibility on the part of the publishers or authors for loss occasioned in any person acting, or refraining from acting as a result of any view expressed therein.

Editorial continued

Concerning the difficulty with the NI number, this is being removed from our new security system which is being designed. Indeed, when it was originally built it was probably an oversight into how to accept entries into this field i.e. accepting all characters in one go, rather than spaced out as presented on a NI card.

As I've just mentioned, we are creating a new system which has been in development now for 18 months and is due to go live before June this year. This will rectify the issues you encountered with the User ID and PIN. With the new system you will be given a User ID and temporary password when you register (the password being issued to you via the post). Once you login to the system you will be able to change both User ID and password on your first access.

As you will be an existing registered user, your existing PIN will have to be replaced by a new password, however you will also have the opportunity to change your User ID at that point.

Finally, concerning the fact that you had to re-register for My Site. I fully agree with the comments made. We are looking into this issue with a view to ensuring that our customers can have only one User ID and password for both areas that contain sensitive information (i.e. about your policy) and areas which contain non-sensitive data e.g. subscribing to email alerts on My Site. This work we are prioritising, but it is being addressed and I will ensure that I raise your views with colleagues so that we can raise the urgency of delivering this to our customers.

My only worry is that did I get this response because I mentioned that I was a technology journalist? I hope not.

Neither was I surprised when I, along with the entire population, was unable to register on-line my newly acquired Sainsbury's Nectar card. The reason that I was not surprised is because I have had problems with the user interface of their store website for years. Try using their store locator. You have to get things just right, No fuzzy logic here. No automatic conversion of lower case into the appropriate upper equivalent. As a search engine it makes the deciphering of the Rosetta stone look like kindergarten work. An example. A few years ago they opened a new store in a village called London Colney which is about 6 miles from where I live. The search engine gives you four options: a post code, a town, a London district, or a county. I enter my postcode and six 'local' stores are listed. None of them the one that I am looking for and some of them further afield. I try entering a town. The nearest town to the store that I am looking for is Saint Albans. No, don't try that spelling it doesn't work. How about 'St Albans'. No that doesn't work either. Neither do lower case equivalents. I cracked it in the end. After 30 minutes of frustration I eventually entered 'St. Albans'. Notice the period after the 'St'? It's absolutely essential to finding the store. Still, a result. Not really. I wanted to check the Christmas opening times. They were wrong! This was two years ago. Yes, I complained. Yes it would be fixed, But it still isn't. I checked it just a moment ago. They still require that period. Thank goodness that Google and Enfish aren't so fussy, otherwise I would never find anything.

Still, enough of my ranting, but I do feel better! Onto the content of this edition. We have a real heavyweight article from Viacheslav Katok on using mathematical modelling techniques to optimally allocate your audit staff, the official BCS response to the Government's consultation paper on entitlement (read identification) cards, a piece from Bob Ashton dealing with recruitment within an ISO 17799 context, reports from Rupert Kendrick on our last two events, some examples of the Nigerian 419 scam and a humour page which is aimed at getting you to write better audit reports.

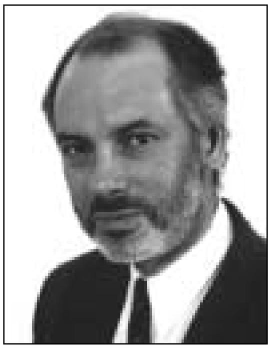
AND FINALLY .... The AGM is scheduled for the 13th May. We are ***desperately*** in need of volunteers for the Management Committee. We are losing our Chairman and Treasurer and need help in organising events. We are the oldest specialist group in the BCS. We are also one of the largest and we have substantial financial reserves, but this will all count for nothing if we can't get enough people to manage it. There is a real danger that the Group will fold unless we receive help. Please do your bit by putting in a little effort. You will find an application form with this edition.

John Mitchell

Chairman's Corner

John Bevan

IRMA needs new officers and committee members for the group to continue. If no members come forward to fill these positions, the group will close. Then one of the oldest, largest, and best financed of the BCS Specialist Groups would no longer organise half a dozen meetings a year for IT auditors and risk managers at bargain prices, and valuable networking opportunities would be lost for ever. At our last members' meeting a few volunteers made cautious offers of help, to plan the programme of meetings for the next season. We also discussed how to solve this problem, and decided that we could probably reduce the workload of a new Treasurer by contracting out the bookkeeping. However, no other bright ideas or solutions emerged. We cannot escape the conclusion that we need a new Treasurer and probably Chairman, as well as at least four new committee members at the AGM in May. I hope that we can convert at least one or two of the cautious volunteers into permanent committee members, but we need more. If you might be interested, please contact me to discuss what is involved. It,s not all hard work. The "perks" include free attendance at all meetings, and building a wider range of professional contacts.



On a lighter note, I think that I may have found the ideal spring or summertime Saturday destination for the IT auditor or risk manager, partner, and children. Those who enjoy shopping can go to central Milton Keynes, whilst others can visit nearby Bletchley Park and its various museums which chart the wartime success of British cryptographers and the rise of British computing. Both locations are well served by train services. Check opening times before you leave home, and write up your experiences for this journal on your return!

Mathematical Programming for Audit Risk Assessment and Scheduling

By Viacheslav Katok

Introduction

This paper describes some research based on using operations research/management science methods for risk-based annual internal audit planning.

The consideration of the method was in relation to large internal audit departments. The bias towards large departments does not mean that planning is irrelevant to small departments, but it was anticipated that if methods could be used for planning purposes they would be capable of dealing with the latter. It becomes usual with internal audit departments to have high level of staffing by aggregating discrete units together. External audit firms are much larger, but their size is spread across a large number of clients and assignments. The type of work also differs between the two audit functions. However, it is expected that smaller departments and external auditors would benefit from the research.

The level of internal audit department performance should be specified by the firm's top management and it is required for the head of internal audit department to submit at least an annual plan for approval by the board, or CEO, and to account for the work done against that plan. This accountability may be fairly easy to discharge if only a few staff are involved, but it becomes increasingly difficult as the number of auditors increase and the head of internal audit department becomes remote from the day-to-day work. This remoteness is increased if the audit department is geographically dispersed and dealing with several divisions within a large company.

Scientific methods and tools can enhance audit coverage by using the minimum amount of resources (efficiency and economy) with maximum effect to achieving of audit objectives (effectiveness). Cutting the time for performing risk assessment and developing an annual audit plan is one of the targets of implementing these methods and tools.

Structuring the Scheduling Problem

Consider the operation of an internal audit department. The organisation employs one or more auditors; each auditor is capable of processing a variety of audit tasks but with different rates (or efficiencies). Also, the internal audit department may be engaged in auditing a number of audit engagements within a given planning horizon. The engagements are received at different points in time within the planning horizon and are expected to be completed at certain dates. Each engagement consists of a set of interrelated steps or tasks, where a task cannot be processed until certain other tasks are completed. The problem the internal audit department is faced with is that of determining a feasible optimal or near optimal operating schedule. The operating schedule, which is the finest form of planning, specifies which audit tasks should be processed, who should process an audit task and when. As the audit engagements increase in complexity and the load of the internal audit department increases or the auditing objectives and emphases change, obtaining feasible schedules becomes a difficult problem, and obtaining optimal or near optimal feasible schedules becomes an even a harder problem, yet one which is very important and common in audit practices. Similarly, responding to any changes in the audit environment and revising the schedules accordingly is necessary, but can be very difficult.

Since one of the main objectives of internal audit is to promote operational efficiency within the organisation, surely the internal audit department must be concerned about the efficiency of its own operations, where efficiency can be measured in different forms. Appropriate scheduling of auditors enhances audit efficiency.

Researchers in audit scheduling have primarily emphasised the issue of loading not scheduling. However, the operating schedule defined above carries more pointed information than a simple loading schedule. From the operating schedule, work profiles can be generated, the auditor's load and utilisation factor can be easily calculated, the schedule of each audit engagement can be easily derived, the impact of the due dates can be assessed, and due dates can be adjusted accordingly. Also, the desires of the individual auditors for processing certain types of audit tasks can be assessed and may be totally accommodated, and the impact of conflicting audit scheduling objectives can be evaluated. Responding to expected and unexpected changes in the information of the auditors or the audit engagements, and revising the schedules can be easily achieved. Naturally, these facilities can greatly enhance the audit planning and control process.

The scheduling problem defined above is neither a job nor a flow shop scheduling problem. The problem can be classified as a the multi-project scheduling under limited resources. Hence, the methods of project planning and control and production scheduling will be extended to this problem. These include the methods of activity networks analysis as well as resource levelling and limited resources methods.

To deal with the audit scheduling problem as a multi-project scheduling problem, first, each audit engagement is treated as a project; hence, it can be broken into a set of interrelated tasks. Then an activity network is used to represent the audit engagement. The networks of the individual engagements can be combined together into a major network which reflects the arrival times of the engagements, the desired processing priorities among the audit engagements and any possible dependencies between the audit engagements. The major networks, besides exemplifying the precedence relations and serving as a communication and controlling tool, is used to test the feasibility of the department involvement and to reduce the number of decision variables in any mathematical formulation for the resource constrained-scheduling problem.

Second, given that each audit task can be processed by different auditors with different efficiencies, i.e. the audit task duration is not a unique constant value, the time analysis used in the Longest Path Method is modified and used to determine how early each audit task can start and how late it can finish. What can be obtained from modified time analysis is a time interval in which the audit task must be completed regardless of who is the processing auditor.

Finally, the preceeding network model may answer some managerial questions, but it does not deal with the issues of loading and sequencing. To deal with these issues the problem is formulated as an integer linear program in which the above time intervals are used to reduce the number of decision variables. The integer program allows testing the impact of different objectives on the operating schedule and the accommodation of all the real life audit considerations. These include the inability of the auditor to process more than one task at a time, precedence relations among the tasks, arrival and due dates, the desire of an auditor to serve a certain client or the desire of a client to have a certain auditor, the desire of the manager to implement a certain training program maintaining a minimum and maximum utilisation factor for each auditor and responding to changes in the information set. The use of integer programming in scheduling is well known in production and project management. But it has not been applied to any real life audit scheduling problem.

The further complication of the problem can be done by adding specific consideration of auditor travel and costs. Travel cost includes airfares and other out-of-town costs such as hotel, car rental, and meals. More specifically, the optimal schedule should provide information on who should travel and when; the number of auditors sent to a given destination; the task that each auditor should carry out at the destination; the length of each auditor's stay; the travelling cost for a given audit project; the total time to be spent on travel; and how, overall, travelling should be arranged so that all the requirements of the audit project will be satisfied and the total audit cost be minimised. Thus, the operating schedule should include the consideration of the travel times as sequence-dependent set-up times, and represents these time-and-cost components explicitly in the scheduling model.

Mathematical Model Description

The Objective Function

The optimal schedule, in addition to its dependence on the constraints, depends on the desired objectives. There are many objectives the organisation can choose from. In this paper the objective function minimises the total cost of:

* mismatching between the auditors and audit tasks, problems faced by many audit departments;

* the total lateness penalty (delay) in the completion of the audit engagements beyond their respective due dates, probems faced by many production scheduling problems;

* travel time as discussed above;

* out-of-town as discussed above.

Therefore, the objective function is to minimise the total cost:

$$W = \sum_{i=1}^{N} \sum_{j \varepsilon J_i} \sum_{k=e_j}^{l_j} C_{ij} X_{ijk} + \sum_{g=1}^{G} \sum_{k=d_g+1}^{T} P_g (1 - Y_{gk}) + \sum_{i=1}^{N} \sum_{(hj) \varepsilon \Delta i} \sum_{k=e_h+a_{ihj}}^{l_j - t_{ij}} A_{ihj} Z_{ihjk} + \quad (1)$$

$$+ \sum_{i-1}^{N} \sum_{\substack{u=1 \\ u \neq u_i}}^{L} B_{iu} \left\{ \sum_{\substack{(hj) \varepsilon \Delta i \\ h \varepsilon L_u}} \sum_{k=e_h+a_{ihj}}^{l_j - t_{ij}} (k - a_{ihj}) Z_{ihjk} - \sum_{\substack{(hj) \varepsilon \Delta i \\ j \varepsilon L_u}} \sum_{k=e_h+a_{ihj}}^{l_j - t_{ij}} (k - 1) Z_{ihjk} \right\},$$

(W - sum of mismatched costs, lateness penalty (delay) costs, auditor travel costs and out-of-town costs), where X_{ijk}, Y_{gk} and Z_{ihjk} are 0-1 decision variables, and others are parameters defined as follows:

If auditor i completes task j at the end of the time period k, where k is the index of the kth time period, k=1,2,3,...,T, with T being the total number of time periods of the scheduling horizon and i and j are defined later

$X_{ijk} = 0$ otherwise

if all the task of engagement g are completed by period k (i.e. completed in period k-1 or before)

$Y_{gk} = 0$ otherwise

if auditor i completes task h then j, and switching from task h to task j requires a non-negligible amount of travel time and the travel ends at the end of period k

$Z_{ihjk} =$ 0 otherwise

The first two components of the objective function, mismatch cost and lateness penalty cost. The third component refers to airfare or transportation cost, which depends on the destination and the class of service used by auditor i. The fourth component refers to out-of-town costs, which depend on the length of stay, the class of service used by auditor i and the out-of-town location. Finally, in setting up J_i (the set of tasks that can be proceeded by auditor i), I_j (the set of possible auditors who can process task j) and C_{ij} (the mismatch cost between auditor i and task j), factors such as auditor's experience, expertise, training, preferences and personalities; and clients' requirements may be taken into consideration.

The objective function can be also added to maximise the total risk coverage, where the objective function to be optimised is obtained by performing a risk assessment:

$$\sum_{j=1}^{N} R_j ,$$

where R_j - overall risk score of an audit task j, j=1,2,3,...N, where N the total number of audit tasks. In this case, the integer programming should be changed to goal programming, but the discussion of its implementation requires a separate consideration.

Definitions and Notations

The following listing of notations is used in the mathematical model description.

C_{ij} - the mismatch cost between auditor i and task j; is the index of the ith auditor, i=1,2,3,...,.N, where N is the total number of auditors assigned to the project; j is the index of the jth audit task, j=1,2,3,...,M, where M is the total number of audit tasks in the project. (Mismatch here is interpreted as the degree of inappropriateness of assigning an auditor to an audit task. The higher the degree, the higher the mismatch cost will be.)

P_g - the lateness penalty cost for each time period past the due date of engagement g; g is the index of the gth engagement, g=1,2,3,...,G, where G is the total number of engagements included in the project network.

a_{ihj} - the number of time periods required for travel when i switches from task h to task j.

A_{ihj} - the travel cost for auditor i switch from task h to task j.

B_{iu} - the out-of-town cost per time period for auditor i in location u; u is the index of uth location, u=1,2,3,...,L, where L is the total number of different locations in the audit project.

N - the total number of auditors.

L - the total number of locations.

T - the total length (number of time periods) of the scheduling horizon.

G - the total number of audit engagements included in the project network.

d_g - the due date of audit engagement g.

J_i - the set of tasks that can be processed by auditor i.

I_j - the set of possible auditors who can process task j.

(hj) - a switch from task h to task j; where h precedes j (a switch is a turning to execute a task after the completion of a previous task).

 - the set of switches that can be done by auditor i; (hj) is feasible for auditor i if and only if both tasks h and j can be processed by auditor i.

L_u - the set of all audit tasks that are in location u.

u_i - the location index of the home office of auditor i. This assumes that all auditors are in their home offices at the beginning and travel back to the same office at the end of the audit. If this assumption is not used, one can define a dummy task at any location where the auditor is supposed to return.

e_j, l_j - the earliest and latest completion time of task j.

t_{ij} - the estimated time required by auditor i to complete task j.

4.2.3 The Constraints

The objective function in equation (1) is to be minimised subject to the following constraints.

Task assignment must satisfy each auditor's availability of time:

$$T_i^- \le \Big\{ \sum_{j \varepsilon J_i \cap L_{u_i}} \sum_{k=e_j}^{l_j} t_{ij} X_{ijk} + \sum_{(hj)\varepsilon\Delta_i} \sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} a_{ihj}\ Z_{ihjk} + \sum_{\substack{u=1\\u\neq u_i}}^{L} \Big[\sum_{\substack{(hj)\varepsilon\Delta_i\\h\varepsilon L_u}} \sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} (k-a_{ihj})\, Z_{ihjk}$$

$$- \sum_{\substack{(hj)\varepsilon\Delta_i\\j\varepsilon L_u}} \sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} k\ Z_{ihjk} \Big] \Big\} \le T_i^+, \qquad (2)$$

for each i=1,2,3,...,N, where T_i- and T_i^+ are respectively, the minimum and maximum time auditor i is available. It is assumed that idle time in a location away from home is counted toward the available time.

B. Each audit task must be completed by exactly one auditor:

$$\sum_{i\varepsilon I_j} \sum_{k=e_j}^{l_j} X_{ijk} = 1, \qquad (3)$$

for each j=1,2,3,...,M, where M is the total number of tasks and I_j is the set of auditors that can process task j.

The audit schedule must satisfy precedence relationships:

$$\sum_{i\varepsilon I_h} \sum_{k=e_h}^{l_h} k\, X_{ihk} + \sum_{i\varepsilon I_j} \sum_{k=e_j}^{l_j} t_{ij} X_{ijk} - \sum_{i\varepsilon I_j} \sum_{k=e_j}^{l_j} k\, X_{ijk} \le 0, \qquad (4)$$

for each h ε B_j and j=1,2,3,...,M, where B_j is the set of tasks that directly precede task j.

D. The time that the terminal task of an engagement ends determines the number of delay periods, thus establishing the relationships between X_{ijk} and Y_{gk}:

$$\sum_{k=e_{j_g}}^{T} Y_{gk} = T - \sum_{i\varepsilon I_{j_g}} \sum_{k=e_{j_g}}^{l_{j_g}} k\, X_{ij_gk}, \qquad (5)$$

and Y_{gk} is a 0-1 variable for each g=1,2,3,...,G, where j_g is the terminal task of engagement g.

E. An auditor cannot process more than one task at any given time. This constraint is referred to as resource levelling, a convention in scheduling literature:

$$\sum_{j\varepsilon J_i(k)} \sum_{q=k}^{k+t_{ij}-1} X_{ijq} + \sum_{(hj)\varepsilon\Delta_i(k)} \sum_{l=k}^{k+a_{ihj}-1} Z_{ihjl} \le 1, \qquad (6)$$

for each k=1,2,3,...,T and i=1,2,3,...,N, where $J_i(k)$ is the set of tasks auditor i can process in period k, and Δ (k) is the set of switches auditor i can do in period k.

F. For a given schedule, from each task there is at most one task for which travel may be involved:

$$\sum_{i\varepsilon(S\cap I_h)} \sum_{(hj)\varepsilon\Delta_i} \sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} Z_{ihjk} \le 1, \qquad (7)$$

for each h=1,2,3,...,M, such that $S \cap I_h \neq \phi$. That is, if $Z_{ihjk} = 1$ for one combination of i, h, j, and k for a given h, then $Z_{ihjk} = 0$ for all other combinations. Here S is the set of auditors who can travel. Without this constraint, there could be more than one travel from task h to some task j in different time periods.

G. For a given schedule, at most one switch to a task may involve travel:

$$\sum_{i\varepsilon(S\cap I_j)} \sum_{(hj)\varepsilon\Delta_i} \sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} Z_{ihjk} \le 1, \qquad (8)$$

for each j=1,2,3,...,M, such that $S \cap I_j \neq \phi$. Without this constraint, there could be more than one travel to task j from some task h in different time periods.

H. For any two tasks in a given schedule, only one task can precede the other between each pair of task so that travel may be involved:

$$\sum_{i\varepsilon(S\cap I_h\cap I_j)} \Big(\sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} Z_{ihjk} + \sum_{k=e_j+a_{ijh}}^{l_h-t_{ih}} Z_{ihjk} \Big) \le 1, \qquad (9)$$

for each h, j=1,2,3,...,M and h ≠ j, such that $S \cap I_h \cap I_j \neq \phi$ (that is, if $Z_{ihjk} = 1$ for one combination of i, h, j, and k for a given pair (hj), then $Z_{ihjk} = 0$ for all i, h, j, and k, and vice versa).

I. Define an auxiliary variable W_{ihj} as follows:

if auditor i completes task h before j

W_{ihj} =

otherwise; this includes cases when (a) auditor i does not perform h, (b) i does not perform j, (c) i performs neither h nor j, and (d) i performs h after j.

The following constraints relate W_{ihj} to X_{ihk} and X_{ijk}, to achieve the preceding definition for W_{ihj}. Note that W_{ihj} is used in constraints J for the determination of:

(a)

$$W_{ihj} \le \sum_{k=e_h}^{l_h} X_{ihk} + \sum_{k=e_j}^{l_j} X_{ijk}, \qquad (10)$$

(b)

$$W_{ihj} \le \Big| \sum_{k=e_h}^{l_h} X_{ihk} + \sum_{k=e_j}^{l_j} X_{ijk} - 1 \Big|, \qquad (11)$$

(c)

$$\sum_{k=e_j}^{l_j} k\, X_{ijk} - \sum_{k=e_h}^{l_h} k\, X_{ihk} + R\Big(\sum_{k=e_h}^{l_h} X_{ihk} - 1 \Big) \le R\, W_{ihj}, \qquad (12)$$

(d)

$$R\,(W_{ihj} - 1) \prec \sum_{k=e_j}^{l_j} k\, X_{ijk} - \sum_{k=e_h}^{l_h} k\, X_{ihk}, \qquad (13)$$

for each i=1,2,3,...,N and (hj) $\varepsilon\Delta$, where R is a sufficient large integer.

J. Travel is involved if and only if an auditor is assigned two tasks, one immediately after another, and switching between them requires a non-negligible travel time. Equations (14) and (15) provide the mathematical definition of travel as explained above:

(a)
$$\sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} Z_{ihjk} = 0, \qquad (14)$$

for each i ε S and (h j) ε J_i, h ≠ j such that $a_{ihj} = 0$.

(b)
$$-R\left(1-\sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} Z_{ihjk}\right) \leq \left\{\left(\sum_{l\varepsilon J_i} W_{ilj} + 2\sum_{k=e_j}^{l_j} X_{ijk}\right.\right.$$
$$\left.-\left(\sum_{l\varepsilon J_i} W_{ilh} + 2\sum_{k=e_h}^{l_h} X_{ihk}\right) - 1\right\} \leq R\left(1-\sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} Z_{ihjk}\right), \qquad (15)$$

for each i ε S and (h j) ε Δ, where R is a sufficient large integer.

(c)
$$\left\{1-\sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} Z_{ihjk}\right\} \leq \left\{\left|\left(\sum_{l\varepsilon J_i} W_{ilj} + 2\sum_{k=e_j}^{l_j} X_{ijk}\right) -\right.\right.$$
$$\left.\left.-\left(\sum_{l\varepsilon J_i} W_{ilh} + 2\sum_{k=e_h}^{l_h} X_{ihk}\right) - 1\right|\right\}, \qquad (16)$$

for each i ε S and (h j) ε Δ .

K. The audit schedule must satisfy sequencing requirements considering necessary travel time:

$$\left\{\sum_{k=e_h}^{l_h} k\,X_{ihk} + a_{ihj}\sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} Z_{ihjk} + R\left(\sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} Z_{ihjk} - 1\right)\right\} \leq \left\{\sum_{k=e_h+a_{ihj}}^{l_j-t_{ij}} k\,Z_{ihjk}\right\} \leq$$
$$\leq \left\{\sum_{k=e_j}^{l_j} k\,X_{ijk} - t_{ij}\sum_{k=e_j}^{l_j} X_{ijk}\right\}, \qquad (17)$$

for each i ε S and (h j) ε Δ, where R is a sufficient large integer.

Constraints A and E, in combination, provide for the constraints on each auditor's available time, the precedence relationships, audit deadlines and delay, and each auditor's assignment to audit tasks. Constraint B requires each audit task to be completed by a single auditor, because audit tasks in an audit project network can conveniently be set up that way. Constraint E prevents an auditor from being overloaded, a feature referred to as resource levelling. If an auditor is allowed to process more than one task at a time, this can be accommodated into scheduling process informally. If there is no delay in completing either task, then there is no change in the original schedule. If there is a delay, the schedule will have to be revised. Constraint E also restricts an auditor to either work or travel, but not both.

Constraints F and K are used to define and regulate travel behaviour. Constraints F and G are used to prevent repeated travel on a path over different time period. Constraint H requires that travel between each part of tasks only occur in one direction. Constraint K assures that the travel time needed in a schedule will not violate sequencing requirements. All of the preceding constraints are linear, except for those with absolute values representing 'either-or' constraints.

Conclusions

The research based on the existing literature on risk assessment and audit scheduling provides the mathematical model for determination of the optimal audit schedule in audit planning. Incorporating into the model audit objectives such as maximising the risk coverage and minimising the total cost of mismatching between auditors and audit tasks, set-ups, delay in the completion of the audit engagement beyond their respective due dates and travel time and costs gives the head of internal audit a chance to make the complicated scheduling process, especially for audits of multinational companies, easily and effectively.

Modelling is a building block process. Exactly how many factors should be included in the model is a cost-benefit decision. For example, the model can be extended to include a time factor in transportation and out-of-town costs that could further reduce travel costs. Another extension can be the consideration of group discount on travel and accommodation.

The optimal schedule provides a general guideline as to how an internal audit project should be carried out. It does not, however, eliminate the need for professional judgement in audit management. Nonetheless, the proposed model is sufficiently versatile as to allow one to incorporate many important audit variables. The model may be used for simultaneously scheduling any number of audit engagements, and for different audit approaches, including the traditional cycle approach and the recently proposed risk-based approach or even cycle-based risk approach. Audit risks can be taken into consideration in estimating auditing time required for each task and in the assignment of auditors. Schedule revisions due to unexpected events such as significant changes in audit time and cost estimates and changes in external environment can be readily made due to the efficiency of the computerised schedule. Similarly, any mis-estimation of the value of model parameters can be easily corrected, and in many cases, the final result is not sensitive to such mis-estimation. Non-audit activities such as attendance of meetings and vacations can easily be incorporated into the scheduling process. These activities can be planned well ahead of time due to advanced knowledge of the auditor's work schedule.

Finally, adequate training for auditors is required before any sophisticated decision science model can be properly implemented. Some trial experiments of the models are also necessary for auditors to gain confidence in the use of the models.

From a more theoretical perspective, the mathematical model extends the theory and methods of cost control by proposing an approach through which a sequence-dependent set-up cost (and time) and a related variable out-of-town cost (and time) can be programmed into an optimisation process for audit planning.

Viacheslav Katok is IT Audit Manager at
Abal Security Ltd. 41 Epsom Road, Morden, Surrey SM4 5PR.
tel: 020 8685 0088, fax: 020 8685 0077, mob: 07798 782198,
email: katok@abalsecurity.com

Bibliography

Adams, J.R. and Martin, M.D. (1982) A Practical Approach to the Assessment of Project Uncertainty. *In Proceedings of the Project Management Institute.* Canada: Toronto. IV-F. pp 1-11.

Adlakha, V.G. and Kulkarni, V.G. (1989) A Classified Bibliography of Research on Stochastic PERT Networks: 1966-1987. *INFOR.* 27/3. pp 272-296.

Anderson, D.R., Sweeney, D.J. and Williams, T.A. (1997) An Introduction to Management Science: Quantitative Approaches to Decision Making. 8th ed. (NY: West Publishing Company).

Anderson, U. and Young, R.A. (1988) Internal Audit Planning in an Interactive environment. *Auditing: A Journal of Practice & Theory.* Vol. 8(1). pp 23-42.

Anonymous. NEOS Guide Optimization Tree. Internet WWW pages, at URL: *<http://www-fp.mcs.anl.gov/otc/Guide/OptWeb/index.html>* (version current at 06 September 1999).

Anonymous. Linear Programming: Frequently Asked Questions. Internet WWW pages, at URL: *<http://www-unix.mcs.anl.gov/otc/Guide/faq/linear-programming-fag.html>* (version current at 06 September 1999). in: USANET newsgroup sci.op-research (06 September 1999).

Antl, B. (1980) Currency Risk and the Corporation. (London: Euromoney Publications.

Balachandran, K.R. and Steuer, R.E. (1982) An Interactive Model for the CPA Firm Audit Staff Planning Problem with Multiple Objectives. The Accounting Review. Vol. 57. January. pp 125-140.

Balachandran, K.R. and Zoltners, A.A. (1981) An Interactive Audit-Staff Scheduling Decision Support System. *The Accounting Review.* Vol. 56. October. pp 801-812.

Barefield, R.M. (1975) Studies in Accounting Research 11: The Impact of Audit Frequency on the Quality of Internal Control (FL: American Accounting Association).

Beale, E. (1968) Mathematical Programming in Practice (London: Pitman Publishing).

Blacker, K. (1998) Automating the audit. *Internal Auditing.* April. pp 30-32.

Boritz, J.E. and Broca, D.C. (1986) Scheduling Internal Audit Activities. *Auditing: A Journal of Practice & Theory.* Vol. 6(1). pp 1-19.

Burke, C.M. and Ward, S.C. (1988) Project Appraisal - Finance Approaches to Risk. *In Cook, N.B. and Johnson A.M., Development in Operational Research 1988.* pp 45-70.

Carsberg, B.V. (1971) An Introduction to Mathematical Programming for Accountants (London: Allen and Unwin Ltd.).

Chambers, A. (1994) Effective Internal Audit: How to Plan and Implement (London: Pitman Publishing).

Chan, D. (1993) Reduce, re-use, reschedule. *CA Magazine.* March. pp 46-51.

Chan, K.H. and Dodin, B. (1986) A Decision Support System for Audit-Staff Scheduling with Precedence Constraints and Due Dates. *The Accounting Review.* Vol. 61. October. pp 726-734.

Chan, K.H., Lam, S.F. and Cheng, S. (1998) Audit scheduling and the control of travel cost using an optimization model for multinational and multilocational audits. *Journal of Accounting, Auditing & Finance.* Winter. pp 67-98.

Charnes, A. and Cooper, W.W. (1961) Mathematical Models and Industrial Applications of Linear Programming (NY: John Wiley & Sons, Inc.).

Crouse, D.W. (1979) Risk Analysis in an EDP Audit Environment. *The Internal Auditor.* December. pp 69-77.

Davis, J.T., Massey, A.P. and Lovell II, R.E.R. (1997) Supporting a complex audit judgement task: An expert network approach. *European Journal of Operational Research.* Vol. 103. pp 350-372

Delisio, J., McGowan, M. and Hamscher, W. (1994) PLANET: An expert system for audit risk assessment and planning. *International Journal of Intelligent System in Accounting, Finance and Management.* 3(1). pp 65-77.

Dodin, B. and Chan K.H. (1991) Application of production scheduling methods to external and internal audit scheduling. *European Journal of Operational Research.* Vol. 52. pp 267-279.

Dodin, B. and Elmaghraby, S.E. (1985) Approximating the Criticality Indices of the Activities in PERT Networks. *Management Science.* Vol. 31. pp 207-223.

Dodin, B. and Elimam A.A. (1997) Audit scheduling with overlapping activities and sequence-dependent set-up costs. *European Journal of Operational Research.* Vol. 97. pp 22-33.

Drexl, A. (1991) Scheduling of Project Networks by Job Assignment. *Management Science.* Vol. 37. December. pp 1590-1602.

Erengus, N.S. and Erengus, S.S. (1998) Optimization-based audit planning: A spreadsheet modelling approach. *Internal Auditing.* July/August. pp 16-23.

Ermoliev, Y.M. and Norkin V.I. (1997) On nonsmooth and discontinuous problems of stochastic systems optimization. *European Journal of Operational Research.* Vol. 101. pp 230-244.

Frolov, V.N., Andreev, I.D. and Chernavin, P.P. (1988) Goal programming for management of regions. (Sverdlovsk: Russian Academy of Science). In Russian.

Gardner, J.C., Huefner, R.J. and Lotfi, V. (1990) A Multiperiod Audit Staff Planning Model Using Multiple Objectives: Development and Evaluation. *Decision Science.* Vol. 21. Winter. pp 154-170.

Garsombke, H.P. and Parker, L.M. (1987) Decision support systems and expert systems: Auditing in the information age. *Internal Auditing.* Winter. pp 20-25.

Gotlob, D., Moore, J.S. and Moore K.S. (1997) Optimizing internal audit resources: A linear programming perspective. *Internal Auditing.* Fall. pp 20-29.

Greenberg, H.J. The Nature of Mathematical Programming. Internet WWW page, at URL: <http://www.cudenver.edu/`hgreenbe/glossary/nature. html> (version current at 06 September 1999).

Greenberg, H.J. Myths and Counterexamples in Mathematical Programming. Internet WWW page, at URL: *<http://www.cudenver.edu/`hgreenbe/ myths/myths.html>* (version current at 06 September 1999).

Greenberg, H.J. Mathematical Programming Glossary. Internet WWW pages, at URL: *<http://www.cudenver.edu/`hgreenbe/glossary/A...Z.html>* (version current at 06 September 1999).

Hein, L.W. (1967) The Quantitative Approach to Managerial Decisions (NJ: Prentice-Hall, Inc.)

Hill, D. (1999) Optimal resource allocation for projects. *Project Management Journal.* June. pp 22-31.

HM Treasury (1988) Government Internal Audit Manual. 2nd ed. (London: HMSO).

Ho, S.S.M. and Pike, R.H. (1992) The Use of Risk Analysis Techniques in Capital Investment Appraisal. *In Ansell, J. and Wharton, F., Risk: Analysis, Assessment and Management.* NY: Wiley. pp 71-94.

Hughes, J.S. (1977) Optimal Internal Audit Timing. The Accounting Review. LII (1). pp 56-68.

Hughes, M.W. (1986) Why Projects fail: The Effect of Ignoring the Obvious. *Industrial Engineering.* 18/4. pp 14-18.

Hull, J.C. (1980) The Evaluation of Risk in Business Investment. (Oxford: Pergamon).

Ireland, L.R. and Shirley, V.D. (1986) Measuring Risk in the Project Environment. *In Measuring Success, Proceedings of the 18th Annual Seminar/Symposium of the Project Management Institute.* Montreal. September. pp 150-156.

Jackson, N. and Carter, P. (1992) The Perception of Risk. *In Ansell, J. and Wharton, F. Risk: Analysis, Assessment and Management.* NY: Wiley. pp 55-70.

Kaplan, S. and Garrick, B.J. (1984) On the Quantitative Definition of Risk. *Risk Analysis.* Vol. 1. pp 11-28.

Kidd, J. (1991) Do Today's Projects Need Powerful Network Planning Tools? *International Journal of Production Research.* Vol. 29/10. pp 1969-1978.

King, R.J (1981) A Practitioner Looks at Auditing Standards and Risk Analysis. *The Internal Auditor.* October. pp. 59-65.

Knechel, W.R. and Benson, H.P. (1991) An optimization approach for scheduling internal audits of divisions. Decision Science. Spring. pp 391-406.

Kramer, J.F. and Nich D.L. (1989) Project management techniques in planning operational audits. *Internal Auditing.* Winter. pp 34-38.

Lam, S.F., Chan, K.H. and Cheng, S. (1998) On the Pitfall of Using Intuitive Judgement in Audit Scheduling. *Advances in Quantitative Analysis of Finance and Accounting.* June. pp 26-32.

Lee, C.F. (1985) Financial Analysis and Planning: Theory and Application (California: Addison-Wesley Publishing Company).

Lee, S.M. (1976) Linear Optimization for Management (NY: Mason/Charter Publisher, Inc.).

Levin, R.I. and Lamone, R.P. (1969) Linear Programming for Management Decisions (Illinois: Irwin).

Levin, R.I., and etc. (1992) Quantitative Approaches to Management. 8th ed. (NY: McGraw-Hill, Inc.).

Littlechild, S. and Shutler, M. (1991) Operations Research in Management (London: Prentice Hall International).

Mao, J.C.T. (1969) Quantitative Analysis of Financial Decisions (NY: Macmillan).

March, J.G. and Shapira, Z. (1987) Managerial Perspectives on Risk and Risk Taking. *Management Science.* Vol. 33/11. pp 1404-1418.

McNamee, D. Risk Assessment Glossary. Internet WWW page, at URL: <*http://www. mc2consulting.com/riskdef.htm*> (last update 03 September 1999).

McNamee, D. A New Approach to Business Risk. Internet WWW page, at URL: <*http://www.mc2consulting.com/riskart3.htm*> (version current at 06 September 1999).

McNamee, D. and Selim, G. (1997) Risk Management: Defining a New Paradigm for Internal Auditor. Internet WWW page, at URL: <*http://www.mc2consulting. com/rskiiarf.htm*> (version current at 06 September 1999).

McNamee, D. and Selim, G. (1998) Risk Management: Changing the Internal Auditor's Paradigm (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation).

McNamee, D. and Selim, G. (1998) Changing the paradigm. *Internal Auditing.* December. pp 6-9.

Merkhover, M.W. (1987) Quantitative Judgemental Uncertainty: Methodology, Experiences and Insights. *IEE Transactions on Systems, Management, and Cybernetics.* Vol. 17/5. pp 741-752.

Mitchell, J.A. (1988) The derivation of a computer system to aid the internal audit planning process in large internal audit department. PhD thesis. City University Business School.

Moder, J. (1988) Network Techniques in Project Management. *In Cleland, D.J. and King, W.R. Project Management Handbook.* 2nd ed. NY: Van Nostrand Rainhold. pp 324-373.

Morris, P.W.G. (1988) Managing Project Interfaces - Key Points for Project Success. *In Cleland, D.J. and King, W.R. Project Management Handbook.* 2nd ed. NY: Van Nostrand Rainhold. pp 16-55.

Naylor, T.H. and Thomas, C. (1984) Optimization Models for Strategic Planning (Amsterdam: Elsevier Science Publishing).

Oakes, M. (1986) Statistical Inference: A Commentary for the Social and Behavioural Science (NY: Wiley).

Patton, J.M., Evans III, J.H. and Lewis, B.L. (1982) A Framework for Evaluating Internal Audit Risk (Altamonte Springs, FL: The Institute of Internal Auditors).

Ritchie, E. (1985) Network Base Planning Techniques: A Critical Review of Published Development. In Rand, G.K. and Eglise, R.W. Further Development in Operational Research. Oxford: Pergamon Press.

Salewski, F., Schirmer, A. and Drexl, A. (1997) Project scheduling under resource and mode identity constraints: Model, complexity, methods, and application. *European Journal of Operational Research.* Vol. 102. pp 88-110.

Shafer, G. (1976) A Mathematical Theory of Evidence (NY: Princeton).

Shapiro, A. and Titman, S. (1990) A Integrated Approach to Corporate Risk Management. *In Stern, J.M. and Chew, D.H. The Revolution in Corporate Finance.* pp 215-229.

Sawyer, L.B. (1998) Sawyer's Internal Auditing (Altamonte Spring, FL: The Institute of Internal Auditors).

Summers, E.L. (1972) The Audit Staff Assignment Problem: A Linear Programming Analysis. *The Accounting Review.* Vol. 47. July. pp 443-453.

Smith, L.A. and Mandakovic, T. (1985) Estimating: The Input into Good Project Planning. *IEE Transactions on Engineering Management.* Vol. 32/4. pp 181-185.

Institute of Internal Auditors. (1992) Statement on Internal Auditing Standards N9 "Risk Assessment" (Altamonte Spring, FL: The Institute of Internal Auditors).

Institute of Internal Auditors. (1998) Standard for Professional Practice of Internal Auditing (Altamonte Spring, FL: The Institute of Internal Auditors).

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

Refereed articles are academic in nature and reflect the Group's links with the BCS, which is a learned institute governed by the rules of the Privy Council. Articles of this nature will be reviewed by our academic editor prior to publication and may undergo several iterations before publication. Lengthy dissertations may be serialised.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication. News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity. Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission. All submissions should either be on double spaced, single-sided A4 paper, e-mail, or in Microsoft Word, Word-Pro, or ASCII format. Electronic submission is preferred.

Submissions should be accompanied by a short biography of the author(s) and a good quality monochrome photograph, or electronic image.

Submission Deadlines

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

The Web Page

Itsbeennicked.com

Andrew Hawker
University of Birmingham

Two mobile phone retailers were at loggerheads recently, with allegations of the "underhand" use of domain names. Customers typing in "**www.phones4you.co.uk**" found themselves browsing the pages of Carphone Warehouse (and still do, at the time of writing). Understandably, this has not gone down well with the rival outfit at Phones4U.

This is not an original trick by any means. A year or two ago, anyone typing in "**www.thelabourparty.org**" would have found themselves looking at a portrait of Charles Kennedy, and a message welcoming them warmly to the Liberal Democrats. This page has long since been withdrawn.

The use and ownership of domain names is opening up some new opportunities for the commercial lawyers, since we all like to take a flying leap from time to time, and type in a best guess, rather than bother to go via a search engine. The BCS is not immune to this. Put "co.uk" on the end instead of "org.uk" and you will find the pages of BCS Limited in Yorkshire, offering a range of IT services. There is no risk of any real confusion, but at the same time it must be useful to be just a typo away from a well-used web site, visited by lots of potential clients.

(By going to IRMA.co.uk, incidentally, you will find details of a Portsmouth-based band described as *"Pop psychonaughts ... A stupendous array of songs 'pysch' toned, in balance between past and future. Four precious pearls, excited by fuzzy guitars, trembling keyboards and space vocal."* Do the committee get up to some things we don't know about? IRMA.org is also spoken for, by the illustrious but much less exciting Illinois Retail Merchants Association.)

There are numerous examples of sites which "slip-stream" by being just a mis-type or two away from famous names. For example, if you mis-key the order of the letters of "hsbc" in "**www.hsbc.com**" you will find various directories for on-line sales, run by other companies. The same happens with "**www.asda.com**" and some permutations of the "Toysrus" site. It is difficult to see any harm in this kind of low-level scavenging for business.

The more important battles centre on the use and ownership of trade names, where people have actually managed to type them in correctly. In the UK, Sainsburys and BT were among several leading names to assert their ownership rights to domain names, in legal proceedings against One in a Million Ltd in 1998. While this helped to settle that it is illegal to "pass off" a domain name where this is clearly intended to mislead or confuse potential customers, there are still quite a few grey areas.

Anyone interested in seeing in a more recent battle in the making should visit **www.easyhypocrite.com**. Having progressed via an unflattering snapshot of a hippo with its mouth wide open, they will find a web site which is putting out a rallying call to all companies which have the prefix "easy" in their names. The alleged villain is the easyGroup. Having prospered with no-frills flying, easyGroup is now diversifying, and wants to assert the right to control the use of "easy" when applied to other commercial activities. The consortium of companies on the easyhypocrite site is having none of this. It is attempting to bring together the efforts of numerous small "easy-" businesses, in staking their claim to trading names which many of them have been using for years. This perhaps shows the Internet both at its best and its worst. The small businesses can use the Net to identify each other, and pool their resources for any legal battles. At the same time, they are only threatened because of the steam-rollering effects of large corporations who have decided that it is time to broaden their branding.

This problem is unlikely to go away, not least because many Internet companies are so notoriously fragile. When Digicash Inc folded in 1999, its "eCash" trademark proved to be one of its most useful assets. (The company was then bought up by eCash Technologies, Inc, which has in turn been swallowed by InfoSpace, Inc, early in 2002). There will always be elements of wheeler-dealing in deciding who acquires or inherits the rights to "e-" words, and in the future we can expect to see more and more of them. Similarly, as the Internet becomes more and more global, there will be increased scope for the misuse of other people's names, whether intentional or otherwise.

As for the BCS, it can take some comfort that anyone who mis-types its initials will be routed immediately to the booking service for the Royal Festival Hall, or the pages of the Broadcasting Standards Commission. Who says we computer types aren't at home with high culture?

Corporate Governance, Recruitment and 17799

Bob Ashton

Corporate governance can be defined as the systems or processes by which entities are managed and controlled. J. Wolfensohn, president of the World Bank has been quoted: "Corporate governance is about promoting corporate fairness, transparency and accountability."

Risk management is a critical element of corporate governance. The object is to ensure that risk exposures are managed professionally. A good definition of risk management is "the use of pro-active management techniques to protect an organization from unnecessary costs and losses".

A little-recognized area of significant, but avoidable, loss is the failure to adopt prudential practices is verifying the credentials of new employees as part of the recruitment process. Although the checking of previous employers' references and academic qualifications has always been understood as good practice, the failure to observe this basic control is all too common. This risk has been addressed in the International Standard on Information Security Management.

ISO/IEC 17799:2000 : Information Technology - Code of Practise for Information Security Management is recognised as a yardstick of good practice in the area of information security management. It is intended to be applicable to all organisations, regardless of type, size and nature of business. Clause 6.1.2 of this Standard requires that verification checks on permanent staff be carried out at the time of job application, including satisfactory character references.

Although this could be considered to be no more than an expression of common sense and professional behaviour, it is surprising how common it is for managers to fail to put this into practise. Even more inexplicable are cases where references have been taken up, but not acted upon.

Managers need to be aware that failure to adopt a prudential approach in this area carries a number of serious risks. Once an unsuitable employee has been appointed, the avoidable penalties to an organisation can run into millions of dollars. Losses will be accrued through sub optimal performances both from the employee concerned and, tragically, from others whose work and moral is impacted. In a country such as Australia, with its strong labour laws, situations such as this can continue for many years, owing to the difficulties employers have in separating unsatisfactory employees. Although many of these losses may be difficult to quantify, they will, nonetheless, be real. Also, the reputations of the organisations and individuals making such appointments will be unfavourably impacted and lead to negative consequences for the employing organisation in the market place.

I am familiar with one organization where the appointment of an IS audit manager was under the control of financial auditors who could fairly be described as "computer illiterate". As any knowledge of information systems and IS auditing had not been necessary in these individuals' career progressions, it did not enter into the job requirements for the new IS audit manager. Members of the selection panel had no IS audit knowledge and were thus unable to discuss the subject. This led to the successful candidate being appointed on the basis of an outgoing personality. This strategy might have succeeded had references been taken up from the applicant's previous employer. This was not done, and after the appointment had been made, it was discovered that the successful candidate had received a series of unsatisfactory performance appraisals over a number of years from his previous employer and was unable to perform his duties in a competent manner. His outgoing personality combined with his lack of knowledge of IS auditing meant that he had a propensity to speak at great length on subjects of which he had little knowledge, causing great embarrassment both within the organisation and with clients. To make matters worse, this person subsequently appointed an IS auditor on the basis of a casual social meeting. Of course, as this newly appointed manager had not been subject to reference checking he did not see the point of applying this discipline to a subordinate. This new IS auditor was then sent to a client from where he had been fired in the recent past. The client demanded his removal from the assignment, bringing the organisation into further disrepute. All this was concealed from the most senior levels of management of the organisation by the skilful upward filtering of information.

Lawyers are increasingly using compliance with 17799 as a starting point for assessing whether good corporate governance has been applied in the area of information security management. Managers need to be aware that they may face personal liability under the Common Law and Corporations Law if they do not implement appropriate policies in the area of recruitment.

The subject of this article may seem to be such a basic control that readers may reasonably question whether it is worth committing it to paper. The answer is emphatically yes. For an example, several years ago, a major Australian bank recruited a CIO from England, who performed his duties in a seemingly satisfactory manner, controlling an annual budget of hundreds of millions of dollars. This continued for a few years until he was recruited by Australia's major telco.

One of the CIO's tasks in his new employment was to address the staff of a research laboratory who had been selected for redundancy, because of a downsizing exercise.

One of the affected staff decided to check the CIO's doctorate thesis, which should have been available online from the university that granted it. It turned out that no doctorate existed, and that this good doctor could not claim to be a doctor at all, but was in fact a former middle manager at IBM UK, who had been given early retirement. He had also made other claims which in hindsight appeared ludicrous, the principal of which was that he had worked with Professor Enrico Fermi on early nuclear research. The latter was quite impossible given his age. Thus two of Australia's largest organisations had been taken in by a con artist. The fact that had appeared to have performed his function in a satisfactory manner did not save either from extreme embarrassment, and can only have been fortuitous.

Although it would appear counter intuitive, it may be that the greater the reputational risk that an appointment carries, then the less likely those making the appointment are to check candidates' credentials. While it may seem inconceivable that "professional" auditors had not bothered to test the veracity of statements in the cases described above for matters which vitally affect their own business, incompetence such as this is by no means confined to the Audit and IT sectors, or to Australia. For example, British Prime Minister's wife and Judge Cherie Blair recently demonstrated very poor judgement in engaging the notorious Australian con man and convicted criminal, Peter Foster, as a financial advisor in the purchase of two flats for her sons. Foster's worthless investment schemes had already ruined the lives of many Australians and this produced considerable press scrutiny. On the other side of politics, former close associate of Margaret Thatcher and best selling author Lord Archer, currently a Guest of Her Majesty and Prisoner Number FF8282, had made many imaginative academic claims in the past, but was never challenged on these until after his conviction for perverting the course of justice.

The biblical admonition that there is nothing new under the sun applies especially to Clause 6.1.2.

Bob Ashton, "Corporate Governance, Recruitment, and 17799," EDP Audit, Control, and Security, March 2003 (30:8): 19-20. (C) CRC Press LLC. All rights reserved. Used by permission

Australian Cybercrime Doubles in 3 Years

Bob Ashton

The 2002 Australian Computer Crime and Security Survey was published in May 2002. The survey was produced jointly by AusCERT, Deloitte Touche Tohmatsu and the New South Wales Police. This year's survey is based on responses from a wide cross section of Australian organisations in respect of the previous 12 months and builds upon two earlier surveys conducted in 1997 and 1999. However, this year's survey now follows the same format as the recently published 2002 CSI/FBI Computer Crime and Security Survey, in order to facilitate the drawing of direct comparisons between the United States and Australia.

The Australian survey has found that although expenditure on information systems security has increased, so has computer crime, with 67% of respondents reporting a computer security incident, twice the level of 1999. Most computer crime went unreported.

Virus and trojan infection were commonplace while data and network sabotage and computer fraud were also reported. The use of trojan software by fraudsters to capture, and subsequently use, the ID and password strings of unsuspecting e-banking customers to empty their accounts is of concern, particularly as the use of encrypting software, namely secure sockets layer (SSL), offers no protection against this exploit. As these trojans are freely available on the Internet, banks will need to give the highest priority to ensuring that additional controls are in place.

The greatest financial losses, however, resulted from the physical theft of laptop computers, this being reported by 71% of organisations. Respondents only quantified the value of the equipment lost and consequent losses, which are likely to be far greater, were not quantified. Organisations are therefore well advised to give policies and procedures governing laptop security the highest priority. This cannot be described as a high tech threat, and adequate safeguards will be easily identifiable.

The standard wisdom was for a long time that threats from internal sources exceeded external threats. This is no longer the case and the survey confirms that in today's Internet connected environment the threat of external attack now exceeds the threat of internal attack. This finding reinforces the need for strong controls over Internet connectivity. The survey also reinforces the advice contained in my article on "Change Control in the e-Commerce Environment" in the January 2002 edition, on the necessity of ensuring that anti-virus software is up to date, and that operating system patches are applied on a timely basis. The authors of the survey refer to this risk on a number of occasions throughout their report.

The Australian survey is available from: **www.deloitte.com.au**

The American survey is available from: **www.gocsi.com/pdfs/fbi/FBI2002**

Assessing and Managing Risk

Who should be doing what - and Why?

Events Reporter, Rupert Kendrick, highlights the key features from an absorbing seminar on Implementing and Auditing IT Governance, promoted jointly with the ICAEW in November 2002

Horace Walpole once said of the US navy, "Everything's at sea except the fleet". In some organisations, everything works except a strategy for managing the risks, which in some cases can impact upon a company's very existence. This event picked up all the disparate threads and drew them neatly together. Delegates attending this event now have no excuse for the absence of a risk management strategy in their organisations!

The event looked progressively at the implementation process from basic concepts, through the role of risk management, the development and measurement of a control environment, the implications of control self-assessment and consequential auditing procedures.

Gary Hardy director, IT Winners Ltd opened the event with a concise outline of IT Governance concepts and the use of Control Objectives for IT (CobiT). He suggested that there are three key issues to resolve:

- Is IT being handled correctly and is the organisation deriving benefit?
- Is the Board offering adequate and effective leadership?
- Is management reaction appropriately on implementation and management?

There are also external pressures to be considered, from both customers and stakeholders,

A 'governance' strategy is essential if an organisation is to understand its strengths and weaknesses adequately. He recommended a 'due diligence' approach, on the basis that an enterprise should be equally inquisitive about itself.

As IT is critical to almost every organisation, it is vital that the Board plays a pivotal part in implementing a 'governance' framework' The driver for the Board's participation will be customer and stakeholder pressure and its responsibility will be to ensure that the IT strategy aligns with business objectives and provides value for money by assisting in managing risk.

Management's role involves implementation, and ensuring the strategy cascades down the organisation, by providing a suitable framework and infrastructure that embeds responsibilities and measures performance.

Auditors try to ensure the Board and management focus on their respective responsibilities and recommends the adoption of a suitable control within a governance programme.

Underpinning the strategies of these functions is the management of risk. It is the Board's duty to manage enterprise risk. The staging posts for this are: the development of risk awareness; the allocation of responsibilities; a recognition that risk management can lead to cost efficiency and competitive advantage; and the embedding of a culture of risk management.

John Mitchell of LHS Business Control and chairman of the event drilled down into the risk management perspective. The foundation for risk management strategies originates with the Turnbull report, which developed the principle that an organisation's annual report should contain a statement that the Board has examined the effectiveness of internal control; namely financial, operational compliance and risk management.

Risk management is the identification of things that must happen for business objectives to be achieved; the identification of events that prevent achievement of objectives and the management of threats that prevent achievement of objectives.

He then identified the components of risk

- inherent risk - the likelihood and consequence of risk crystallisation before controls had been put in place;
- residual risk - the likelihood and consequence of risk crystallisation after mitigating controls have been put in place; and
- retained risk - the level of risk formally accepted by the organisation (usually the same as residual risk).

Risk can be terminated; transferred (e.g. insurance); tolerated or treated. Delegates were taken through a series of complex scenarios for handling risk, each of which were thankfully simplified by an explanatory matrix. Control, he emphasised, can only reduce either the likelihood or the consequence, but not both and a key feature of risk management involves embedding monitoring factors that confirm that the mitigating controls are working effectively.

Anna Writer, senior auditor, BAA plc, looked at the importance of the control environment to the process of managing risk, how it can be measured and how the result can help determine the depth of audit coverage. A 'control environment' is a platform from which the business pursues the objectives and overall strategy. If the platform is strong, the business is more likely to be successful and achieved the planned targets. This involves checking:

- resources;
- systems;
- processes;
- culture;
- structure and strategy.

The speaker drew on the appendix to the Turnbull report, which asks whether objectives are clearly and effectively communicated, whether the company's culture supports risk management and whether the company's policies support a climate of trust. She identified communication as a key strategy in drawing these elements together.

The role of the audit, she explained, was to identify where resources should properly be directed and to what extent resources should be directed to address a specific issue. She concluded that there were three key methodologies for adoption of an effective control environment - questionnaires to staff; commentary and advice; and a CSA - or Control Self Assessment.

Keith Share, compliance manager, Group IT, BAA plc., picked up the question of control self assessment from the previous speaker and provided an insight into the practical aspects of introducing control self assessment into a large and diverse IT department, using BAA as a case study. BAA is located world wide in 10 major and 60 minor locations and is concerned with airport operations that include retailing, consultancy, transport and property development and management.

Reminding delegates of the Turnbull principles, he explained that the mission of the audit was to provide an independent assessment about the effectiveness of BAA's risk management strategy and to identify key improvements that would increase profitability. There were four key aspects to the audit procedure:

- reviewing the effectiveness of the risk management strategy;
- producing balanced and objective reports;
- avoiding conflicts of interest and undue management influence;
- demonstrating commercial awareness of management concerns.

He identified three types of audit procedure. Attestation - evaluates the adequacy of the managements' risk and control mechanism and reviews the process of reasonableness. Confirmation - evaluates the reliability of management's assertions and checks the completeness and accuracy of output. Direct - places no reliance on management's assertions and is used for new business or risk areas.

He then turned to what he termed 'the principle of trust'. Auditors must ask themselves on what basis they trust their client. Is it based on the strength of the control environment or on previous audits with strong internal controls? He summed up the auditor's role as 'we trust, but reserve the right to verify.'

Gabriel Lung, senior auditor, Group Internal Audit, BAA plc., gave the final presentation. He rounded off the day by illustrating how the use of control self assessment by the IT function changes the audit approach and improves the efficiency and effectiveness of the organisation.

He defined control self assessment as a process which allows managers to identify and document the controls in place to mitigate risk and to be able to assess the effectiveness of those controls. This takes place by periodically running the CSA so that managers can determine its effectiveness. Completed CSAs are then passed to Internal Audit for independent testing.

The strategy involves using the risk register as a starting point and then creating a CSA pack and planning strategy. The target audience is identified and a soft copy is distributed. Responses are collated and reviewed until satisfied. A peer group review takes place and the final stage is appraisal by internal audit.

The risk owner, he pointed out, is not necessarily best placed to comment on internal controls, because, for instance, governance issues may cover overall management of IT operations and programmes and projects.

He suggested that a CSA should provide a number of tangible benefits according to BAA's experience:

- focus on managerial responsibilities
- risks and controls are documented
- there is a history of risk and control improvement (or not)
- managers can assert that risks are being controlled
- the company can meet the requirements of Turnbull
- scarce audit resources are freed up.

He ended by suggesting that once fully developed and tested, risk registers are subject to very little change and the CSA becomes a tool for routine review. BAA plans to develop CSAs for statutory compliance issues, such as data protection and BS 7799 and CSAs are embedded in policies and procedures.

This event was excellent value for the delegate fee, and the plush surroundings of the Chartered Accountants' Hall were very conducive to what proved to be an informative and enjoyable event.

Cybercrime Uncovered

Events Reporter, Rupert Kendrick, outlines the key issues arising from this event, held at the Old Sessions House, Clerkenwell Green, on 28 January 2003

It is a fairly safe bet that sets of startling statistics, especially statistics relating to other commercial enterprises, will grab attention. This certainly proved to be the case where the opening presentation at this event, from Chris Potter, PriceWaterhouseCoopers, revisited some of the worrying findings of the Information Security Breaches Survey 2002 (ISBS).

Some 40 delegates had gathered to see just how the rising incidence of 'cybercrime' was developing and how the latest trends might affect their businesses. The seminar looked at a wide range of 'cybercrime'-related issues: computer crime; vulnerability management; forensic computing and legal issues.

The ISBS 2002 did not make for very encouraging reading. Some of the key findings were:

- the number of UK businesses suffering a malicious security incident has doubled since 2000;
- the rise is due primarily to virus infection; hackers; and employee misconduct;
- the threat balance is moving from internal to external;
- viruses are becoming more sophisticated;
- the number of UK businesses with security policies has doubled since 2000, but is still only 27%;
- less than half of UK businesses are addressing data protection compliance.

Copies of the ISBS 2002 were supplied to delegates who were able to discuss the Top Ten (recommended) Actions for the Board:

(i) create a security aware culture;

(ii) have a clear, up-to-date, security policy;

(iii) assign appropriate responsibility to those with appropriate knowledge;

(iv) evaluate return on investment;

(v) build security requirements into designed IT systems;

(vi) maintain up-to-date technical security defences;

(vii) ensure compliance with regulatory requirements;

(viii) develop contingency plans for security breaches;

(ix) understand the application of insurance cover for incidents;

(x) test compliance with the security policy.

Clive Carmichael-Jones, Vogon International, and author of *The Enemy Within*, reviewed the current status of computer crime. He was clearly very knowledgeable on the subject and it was therefore unfortunate that he felt the need to devote the first quarter of the presentation to statistics and details of Vogon International.

He followed with a series of routine facts on the categories of criminal and civil case that Vogon investigated - then more statistics on Internet data growth, disk storage, and the shipping of drives and the use of the Internet - without really explaining how this data applied to the incidence of 'cybercrime'.

There were some general references to the increasing sophistication in the methodology of cybercrime and the problems arising from jurisdiction. However, considering the presenter's background and the research undertaken for his publishing achievements, it was a shame that there were no examples of hard and fast case studies accompanied by guidance for delegates on how to combat the different types of 'cybercrime'.

Peter Wood, of First Base, Penetration Testing Specialist, was clearly on top of his game for this presentation which he delivered with an engaging mix of humour and serious comment. This presentation was certainly for IT specialists. He began by outlining a series of strategies for performing 'ethical hacking'.

These included: browsing for shared 'c' drives; null sessions and targeting computers for administrators' lists and typical passwords; cracking password files; and more direct methods such as keystroke capture analysis - in respect of which he mentioned the KeyGhost solution (www.keyghost.com) - where the user's key strokes can be captured for behaviour detection. Other methods included scanning and dictionary attacks and indirect password cracking.

He ended with some key principles for minimising exposure to vulnerability:

- prevention is better than cure;
- monitor alert notifications;
- monitor logs and reports;
- install an intrusion detection system;
- ensure good physical security;
- train IT staff adequately;
- develop and enforce policies and procedures with drive from senior management and widespread promulgation, supported by education, training and testing.

Clive Carmichael-Jones returned to deliver a second presentation, which focussed on Forensic Computing. He began by outlining the circumstances in which premises are entered - search warrant; search and seize, and management authority. He reminded delegates of the guidelines of the Association of Chief Police Officers over these situations:

- no action should be taken that might change data;
- only competent specialists should access data on a target computer;
- an audit trail should be maintained for verification by independent inspection.

These guidelines are designed to eliminate data change or corruption and exposure to accusations of tempering. In preserving evidence, he stressed the importance of 'imaging' by taking a complete copy of the disk, a well established technique, accepted, he said, by the courts. The image is crucial and is the sole and most reliable evidence available

This was a timely event, given the topicality of the subject and the need to be reminded that 'cybercrime' and the management of information risk are closely connected. The venue was comfortable and the atmosphere relaxed. Delegates should have found this an informative and enjoyable day.

Response from The British Computer Society to the Government Consultation Paper on Entitlement Cards and Identity Fraud

This paper was prepared by the BCS's Security Panel in response to a request by HMG for comments on a proposal for what is effectively an identity card - Ed.

INTRODUCTION

In responding to the Government White Paper 'Entitlement Cards and Identity Fraud' the British Computer Society has not addressed any Governmental or Political issues. This response deals solely with the feasibility of implementing a complex system to allow accurate identification of individuals who are either citizens of the U. K. or who are living and working in the U.K. and seeks to identify practical issues that may arise and require careful management if the risk of project failure is to be reduced.

Although superficially presented as an Entitlement card system with an objective of reducing fraud in the public sector, the consultation paper is, in fact, proposing a far wider and more complex system. The detailed proposals in the document suggest that the system will also support:

* Passport card production
* Proof of Age
* Electoral Register
* New ways of voting
* Personal medical information
* Reduction of crime and reduction of some administration processes in the Police force
* Access by third parties to use the smart card chip to store and retrieve data
* Access by Customs and Excise and the Police to assist in cases of serious crimes

This range of objectives will significantly increase the risk of project failure. Experience has shown time after time that project success is most easily achieved if the project objectives are kept simple. If this project goes ahead it should focus on the core objective of reducing public sector fraud. Once the system is installed to achieve that objective then subsequent projects can be started to meet the subsidiary objectives listed above. This type of project phasing allows management attention to be focussed on simple achievable objectives and will significantly reduce the risk of project failure.

In addition the following links are proposed in order to support the validation and issuing process:

* Interface to the UK Passport Service's passport database
* The passport database operated by the Foreign and Commonwealth Office for the issue of passports to U.K. citizens overseas
* DVLA's and DVLNI's driver databases
* On-line records of births and deaths (if available)
* The central index which holds national insurance records
* Systems operated by the Immigration and Nationality Directorate of the Home Office to check details of those applicants who are foreign nationals
* Possible link to credit reference agencies for name and address validation.

Every effort should be made to reduce this list. Each separate interface is an increase in project complexity leading to a higher risk of project failure. One data source should be selected as the prime system validation source. If further validations are required then they should be performed manually.

A further complication that is not addressed by the consultation document is the impact that this proposal could have on the current drive for e-government.

There is currently a requirement to provide government services on-line where appropriate and there is a demand. The target date for this is end 2005. This is leading to a situation where some Local Authorities are currently investing in local versions of an identity scheme. Clearly this is a duplication of the intent of this consultation paper and some co-ordination is required to avoid unnecessary expenditure on systems that could have a very short lifetime.

DETAILED COMMENTS ON A POINT BY POINT BASIS

P1 (page 16)

The Government invites views on the principle of establishing an entitlement card scheme as a more efficient and convenient way of providing services, tackling illegal immigration and illegal working and combating identity fraud.

If this project is to succeed it must have clearly defined and agreed objectives owned by the senior user management of the department(s) who will be charged with implementing the scheme.

Paragraph 3.9 on page 29 identifies that identity fraud is estimated to cost the UK £1.3 billion each year split equally between the public and private sectors. As one of the golden rules of successful project management is 'keep it simple' this project should only address the management processes that are directly under the control of the User management who are implementing this new system.

This means that the benefit that should be addressed is the £650 million of costs involving identity fraud in the public sector.

Unfortunately the consultation paper does not make clear how those £650 million p.a. savings will be achieved as a result of the introduction of an entitlement card.

This is a significant omission as the project scope cannot be focussed on the primary goal of achieving that saving without this clear linkage. As a result there will be significant 'scope creep' as the project progresses and differing User expectations and opinions are expressed on how the savings can be achieved.

The term 'scope creep' is used to identify the situation where the original project definition changes as the project progresses. These changes can be either in the functionality being provided or the amounts of data being processed and, usually, is a mixture of both. The issue with scope creep is that the original project budget will obviously be inadequate to deal with a situation where the functionality or data needs increase; this is the factor that leads to many ICT projects needing increased budgets from the initial estimates. Avoidance of scope creep is difficult but the primary rule is to endure that the project objectives are simple and understood from the start of the project. Adherence to those initially defined objectives is the best guarantee of avoiding scope creep and budget overruns. This project does not clearly identify how the savings are to be achieved, without that definition the project objectives cannot be stated clearly and unambiguously. The inevitable consequence is that the objectives will change over the life off the project; this will cause budget overruns and project delays. This has been demonstrated time after time in both the public and private sectors.

Taking the text of P1 above the objectives of this project are seen to be:

* More efficient and convenient way of providing services,
* Provide a mechanism for tackling illegal immigration and illegal working
* Provide a mechanism for combating identity fraud (in the public sector).

There is no doubt that the technology exists to allow the introduction of an Entitlement Card, the real issues are:

* Can the project be successfully completed within the current time frame and cost estimates
* Will the introduction of Entitlement cards allow £650 million of savings to be generated within the public sector

The first of these points will be debated in this response and many comments are made in the following. However, the second point cannot be addressed by an external agency. It is the responsibility of the User department responsible for achieving the benefits arising from a new Information Technology (I.T.) project to implement the management disciplines necessary to achieve the objectives and benefits of the new system or process.

Many projects fail because this responsibility is misunderstood.

The failure of the Consultation Paper to clearly identify how the issuing of Entitlement cards will result in a £650 million p.a. saving indicates that this responsibility is not understood here and, therefore, this project will probably fail.

From a Local authority perspective the availability of a national system for validating an individual's identity will allow significantly more efficient and convenient ways of providing services.

P2 (page 17)

Should the Government give consideration to one or more targeted entitlement card schemes and if so what sort of scheme should be considered?

Entitlement cards targeted at specific fraudulent activities would have the benefit of possibly having a far clearer focus and project objectives than a single scheme covering all U.K. citizens. However, there are several issues that must be considered:

* Multiple schemes may end up duplicating administration processes
* Citizens may be issued with more than one card if they fall into more than one target group
* Attempting to integrate the schemes (if ever required) would be a costly and complex process.

If the project objectives were clear and the linkage between the £650 million p.a. savings and the issuing of Entitlement cards clearly defined then a single targeted scheme concentrating on the saving of that £650 million would be the ideal solution from an IT perspective. The project could be structured properly with clearly defined objectives and scope and an owner (User Project Manager) charged with achieving the identified savings.

However, without the certainty and clarity of an understanding of the relationship between the £650 million p.a. and Entitlement Cards it is almost inevitable that any scheme (whether targeted or not) will fail to generate the level of savings expected.

P3 (page 19)

Views are invited on whether the Government should implement a voluntary entitlement card scheme.

The decision as to whether the scheme should be voluntary, universal or compulsory is primarily a political one and the British Computer Society has no comment to offer other than to note that achievement of the benefits will be made easier as the number of people on the scheme increases.

P4 (page 20)

Views are invited on whether the Government should implement a universal entitlement card scheme where:

* **It would be a requirement that all lawful residents of the UK over a certain age register with a scheme and obtain a card.**
* **Service providers would be free to decide whether or not to use the card scheme as the means to access their services.**
* **Service providers who did choose to use the card scheme would make the scheme the exclusive way to access their services (with exceptions for emergencies such as lost or stolen cards)**
* **Some services would rely on the database which administered the card scheme rather than require production of a card if that was a more efficient and convenient way to provide the service**

As noted in the response to P3 the decision as to whether the scheme should be voluntary, universal or compulsory is primarily a political one and the British Computer Society has no comment to offer other than to note that achievement of the benefits will be made easier as the number of people on the scheme increases.

It is very difficult to comment sensibly on the other three points as the consultation paper suggests several ways that a service provider might use the card scheme. The consultation paper suggests that data will be held in three different places (table 5.2 on page 62):

* Visible on the card
* Stored on the chip on the card
* Stored on the central database

This table suggests that all of the data shown on the card will be held in the central database. Unfortunately there does not seem to be a definitive statement as to which data will actually be held in the smart card chip. The simplest option would be to ensure that the data encoded on the card is automatically maintained on the central database and that only a sub set of this data actually appears on the card. Quite apart from any other consideration this approach would simplify the process for managing lost or stolen cards.

One of the most significant issues with computer systems is designing them so that they can be enhanced with minimal cost as requirements change. Given the core objective of this project, which is to save £650 million p.a. of taxpayer's money, the optimum solution would be to ensure that the data necessary to achieve this saving is encoded on the card and stored on the central database. Any other data peripheral to this core objective would be held only on the central database. If service providers then wish to include the use of the card in their processes the central database could be also used to store their data which would not be maintained on the card itself. This would ensure that the card data format remained standard, a simplification that would keep costs down.

Analysing how service providers might use the card in their processes reveal four possible scenarios:

* The service provider simply uses the card as proof of identity and does not attempt to either read the data on the card or access any data held on the central database. There are no technical issues in this scenario.
* The service provider reads the data held on the card. The capability to do this will require clear and consistent data format standards which would be published to allow the service provider to obtain the necessary reading device and write the necessary software. If the card contains data which is deemed to be personal (e.g. medical records) then the situation becomes more complex, as the appropriate encryption routines would need to be employed to prevent unauthorised access to that data. This would increase the cost of the project dramatically as cards would have to be re-called and re-issued to reflect advances in encryption and, perhaps more importantly, de-encryption routines. There may also be Data Protection issues as the card holder may not want to disclose some data on the card (e.g. address or age) to the service provider, so a mechanism for the card holder to determine which data could be accessed by the service provider would be required. Again this would probably result in a significant cost escalation as a result of the increased complexity.
* The service provider does not access the data on the card but uses a call centre to obtain confirmation of data relating to the cardholder with his/her permission. This could be implemented relatively cheaply using the PIN approach that is already in widespread use.
* The service provider directly accesses the central database. This is probably the most expensive of the four options as well as introducing the biggest security issues. Allowing third parties to access the central database will require a dial-in capability with the consequent risk of unauthorised criminal access. Ensuring that the security is in place to minimise that risk will be expensive both at implementation and on an ongoing basis. Allowing authorised access by the service provider will in itself raise security issues, as each service provider would probably only be authorised to access a (different) sub set of the data held on the central database. This will result in complex rules having to be included and supported within the system - an expensive option.

As there are at least these four different scenarios it becomes difficult to be prescriptive as to whether or not a service provider must use the card as the only way that their services may be accessed. In fact it is difficult to think of a rigorous definition that could be used to identify those organisations that will be 'service providers' in this context. A more appropriate approach may be to state that if a service provider required proof of identity then the entitlement card must be accepted as that proof of identity.

P5 (Page 22)

Views are invited on what the contents and scope should be of any legislation to implement an entitlement card scheme.

The primary legislation should cover the following points:

* Clear definition of an individual's rights to verify any data held against him/herself whether on the card or in the central database. The mechanism used for this process and the service level commitments need to be defined.
* Clear definition of the process an individual would use to ensure that incorrect data held against him/herself was corrected.
* The issue of third party access, whether by service providers or external government agencies, requires definition covering such areas as rights of access, specific data items that can be accessed, etc.
* The issue of non-UK government agency access should also be covered. It is not clear form the consultation document whether non-UK governmental agencies (e.g. the U.S. F.B.I.) would be allowed access.

These issues need to be addressed so that a clear definition of the I.T. project scope is achieved. One of the biggest factors in I.T. project failure is 'scope creep' where the project scope continuously changes causing delays and budget overruns.

P6 (Page 23)

Views are invited on what powers the Government should have to require cards to be held in any universal scheme and what incentives and sanctions there could be to help ensure universal coverage.

These issues are primarily political ones and the British Computer Society has no comment to offer other than to note:

* Achievement of the benefits will be made easier if there is a consistent and universal usage of the cards.
* Providing benefits to cardholders (discounts, introduction of appointments systems to remove queuing, etc) will encourage a near universal take up.

P7 Page 25

Views are invited on whether any entitlement card scheme should allocate a unique personal number to each card holder, what form any such number should take and whether it should be incorporated onto the card itself.

A unique personal number will be a pre-requisite for the proposed system to function efficiently. The real issue is whether an existing number can be used or if a new number is required. The obvious contender from the existing numbers in use is the National Insurance Number that should give a unique identification to each U.K. citizen. However, non U.K. citizens resident in the U.K. would not have one of these numbers but would need to be registered on the Entitlement Card system. This suggests that a new number is required. A possible solution would be to use the existing National Insurance Number where possible and to issue new numbers to the same format for non UK citizens. However, care must be taken to ensure that a convention is adopted which does not result in parts of the number having an inherent meaning. This is one of the commonest mistakes that are made in designing new computer systems and leads to a high degree of inflexibility. Whatever number is chosen it should be visible on the card as well as being encoded on the card and held as the primary key on the central database.

P8 Page 26

Views are invited on the development of a national population register which could be used in a sophisticated way across the public sector with the aims of improving customer service and efficiency.

The key question to answer is whether the creation of an accurate and well-maintained central population database would help achieve the £650 million p.a. saving that is the objective of introducing the Entitlement Card.

The implication is that it is not required to achieve this saving; consequently it should not be attempted until after the first implementation. This will keep the initial project as simple as possible and reduce the risk of scope creep and project failure.

The implementation of the Entitlement Card will require the creation of a single database of cardholders, which will form the base for the creation of a National Population Register. The project to create this could then be addressed as a discrete project with its own specific objectives.

P9 Page 29

Views are welcomed on whether an entitlement card scheme would allow for more efficient and effective delivery of Government services and what services people would most like to see linked to a card scheme.

The consultation paper identifies £650 million p.a. saving as the primary objective for the introduction of Benefit Entitlement Cards. The achievement of this objective must be the primary aim of the I.T. project. Attempts to widen the project scope at this stage will lead to an I.T. project failure as the project will simply become too big and complex to manage effectively.

The design objectives for the Benefit Entitlement Card System should reflect the need to extend the project scope once the cards are implemented and the system and the database should be designed with this in mind.

Other design issues that should be considered very carefully are scalability and security.

Scalability is an issue because this will inevitably be a phased implementation (the White Paper suggests a time period of 6 years) and the system must be able to scale up to the 67 million individuals who will be covered by the card system at the end of the implementation period. The technical design required to meet acceptable service levels for such a large number of database entries will not be simple.

Security is an obvious issue as the central database must be extremely secure to deter criminal access whilst having the flexibility to allow partial access by trusted third parties as the various service providers are identified and integrated into the system.

As noted earlier the eventual availability of a national database for identity validation will be of significant benefit to local authorities in their delivery of local e-government functionality.

P10 Page 29

Views are also welcomed from organisations providing services in the public and private sectors on whether they would like to link their services to a card scheme and what features they would want to see in a card scheme that would most benefit their services.

As previously noted the Entitlement Card would be of significant benefit to Local Authorities as proof of identity for service delivery.

P11 Page 31

Views are sought on whether an entitlement card scheme would be a cost effective additional measure against identity fraud and related criminal activities such as money laundering.

As the British Computer Society has no expertise in these areas it is unable to comment.

P12 Page 33

The views of employers, trade unions and other interested parties are sought on whether an entitlement card scheme would be an effective measure (as part of a wider package) to combat illegal working and illegal immigration and what suggestions they might have for how a scheme could be designed to minimise administrative burdens on employers.

The British Computer Society has no direct experience of either illegal working or illegal immigration so cannot comment in that context.

However, it must be noted that attempting to design a system to cope with various third parties' administrative systems will be extremely expensive and complex. A far better approach would be to define the data that is required to address the necessary functionality and then deliver that data in a standard and secure format.

P13 Page 34

Views are sought on whether an entitlement card should be available to UK citizens in a form which allowed it to be used as a more convenient travel document to Europe than the passport book.

As noted in earlier responses this is another example of scope creep. The underlying objective is stated to be saving £650 million p.a. in benefit entitlement fraud. Focus must be kept on this objective if the project is to succeed. Whether the entitlement card subsequently becomes a travel document must be regarded as a subsidiary objective which will only be addressed once the primary objective has been achieved.

P14 Page 36

Views are sought on whether an entitlement card would be an effective proof of age card, whether there should be a minimum age at which entitlement cards should be available and if so what that age might be.

From a system development and operation perspective standardising processes reduce cost. Consequently as long as there is only one rule for whether the date of birth is shown on the card and when the card is issued to a U.K. citizen it does not matter at what age that occurs. Creation of a multiplicity of rules to cater for differing views on whether to show the date of birth and when to issue the card will only increase complexity and cost and increase the risk of failure.

P15 Page 37

Views are sought on

* **Whether an entitlement card scheme would be effective in reducing crimes other than those related to identity fraud**
* **Whether an entitlement card would reduce administrative burdens on the police**
* **Whether the police, intelligence services and other organisations investigating very serious crimes such as Customs and Excise should have access to the central register - including biometric information - in closely prescribed circumstances in cases where they are investigating matters of national security or very serious crimes and what those safeguards should be.**

The British Computer Society has no views to offer on the substance of these proposals.

However, it should be noted that if the third parties identified here (Police and Customs and Excise) ask for specific functionality to be provided then this would be best left until after the primary objective of this scheme had been achieved. As noted in earlier responses the potential for project scope creep in this project is very significant and if not managed carefully will inevitably lead to major overruns in both cost and elapsed time.

P16 Page 38

Views are invited on whether an entitlement card scheme would benefit the maintenance of the electoral register and facilitate new ways of voting.

Of the 67.5 million people who would eventually be issued one of these cards only around 60 million would be UK citizens and therefore eligible to vote. Including functionality in the system to identify entitlement to vote should not be included in the first implementation. This would be a classic example of project scope creep, which would detract from achieving the primary objective for the system. Once implemented an extension of the system to facilitate maintenance of the electoral roll could be managed as a separate project. Phasing the project in this way will result in a faster and cheaper overall implementation.

Using the card to facilitate new ways of voting would require some mechanism to ensure that electoral confidence is maintained in the principle of the secret ballot. Using the card to establish identity for voting purposes would probably be accepted; using the card to enter a voting system may not be so acceptable. This would have to be taken into account in the design of any I.T. based system for voting.

P17 Page 38

Views are sought on:

* **Whether an entitlement card should display emergency medical information and/or act as an organ donor card at the card holder's consent?**
* **If so, what sort of emergency medical information would be most useful to display?**
* **Given space constraints on the card, whether storing emergency medical information on a smart card chip on an entitlement card would be useful?**

Tailoring the card to display variable information on such things as emergency medical information or organ donor decisions (point (i)) will introduce complexities in the card issuing process and will increase the data needed to be held in the central database. Attempting either of these in the first implementation will detract from the primary objective for this project and will increase cost and implementation time scales. A clear assessment of the increased benefits that could be achieved needs to be performed to determine whether the increase in project risk is acceptable.

The British Computer Society cannot comment on point (ii)

Storing emergency medical information on the chip (point (iii)), introduces significant new security issues as the requirement has presumably now been introduced that only certain authorised service providers can access and read certain data held on the chip. This will inevitably lead to increased project costs and time scales. A clear assessment of the incremental benefits that are achievable from this increase in project scope and functionality will be required before the decision can be taken to accept the increase in project risk. A lower cost approach that would introduce less risk would be to only hold this data on the central database and to use wireless devices to access the data in emergency situations. This approach would also remove the need to display variable medical information on the card itself (point (i)). Even with this approach this functionality should be treated as a separate project that would only be started once the prime objectives of this project (saving £650 million p.a.) are achieved.

P18 Page 42

The Government invites views on the early steps it would like to take to tackle identity fraud and welcomes expressions of interest from the private sector to collaborate in this work.

The proposed Identity Fraud Forum contains too many members to allow the necessary clarity of purpose to be maintained for the ambitious project being proposed. A short list of specific project objectives needs to be agreed and then the responsibility for their achievement delegated to a small authoritative team to achieve them. A Steering Committee of project sponsors (no more than 6) should monitor progress. Involvement of the private sector at the steering committee or project management level should be discouraged unless there is a contractual arrangement committing the parties involved to either specific service levels or specific objectives.

The specific proposal to use credit reference agencies to validate address information is a decision that should be taken by the project management team once it has undertaken a review of all of the possible options.

P19 Page 43

Views are invited on whether checks on applications for passports and driving licenses should be strengthened to the degree outlined in Chapter 5 whether or not the government decided to proceed with an entitlement card scheme based around these documents

The British Computer Society has no comments to make on this point.

P20 Page 43

If more secure passports and driving licences were issued around a common identity database shared between the UK Passport Service and the DVLA, the Government invites views on:

* **Whether it should take the necessary legislative powers to allow other departments to access the identity database to allow them to make their own checks.**
* **Whether it should allow the private sector to access the identity database provided this was done with the informed consent of subjects.**

The British Computer Society has no direct comments to make on these points, as they are primarily political decisions. There are, however, implications that would follow if the decisions were taken to allow this type of access.

The necessary system infrastructure could be developed and implemented to support this access. The issues that would need careful consideration relate to scalability and security. In particular allowing third party access to the identity database would require significant investment in security to prevent unauthorised third party access.

There may be a need for a significant 'data cleansing' activity to ensure that the two agencies' data is synchronised correctly.

P21 Page 43

Views are sought on whether the Government should procure a service from the private sector which checked applications for services against a number of databases used by the credit reference agencies or similar organisations and selected biographical data held by the Government.

The following issues would need resolution in this scenario:

* Ensuring that the private sector data was accurate
* Ensuring that all participants in the process were using an appropriate level of security (presumably specified by the Government)
* Adequate mechanisms were in place to assure acceptable response times, even in those situations where one or more of the third party databases were not available.
* Mechanisms could be made available to de-duplicate identities from the third party databases with the associated task of ensuring that data was cleansed and synchronised successfully.
* Adequate scalability was provided as the number of citizens covered by the process increased.
* An agreed audit trail could be produced for problem resolution processes.

Resolution of these issues will probably require a significant increase in project cost.

P22 Page 44

Views are invited on whether a summary-only offence of identity fraud should be created

The British Computer Society has no comments to make on this point.

P23 Page 47

Comments are invited on whether any entitlement card scheme should be based around a passport card and the photo-driving licence (including a non-driving licence entitlement card). In particular, comments are invited on whether having a family of cards rather than a single card would be helpful or confusing. Suggestions of other models for an entitlement card scheme are also invited.

This project is already very ambitious. The intent is to issue an entitlement card to all people resident in the U.K. over a specific age. This is estimated to be 67.5 million people (paragraph 5.39 on page 64). Collecting and validating the required data will be a significant task in itself. Attempting to validate that data against existing data and resolving differences during the collection process will introduce significant delays and vastly increase the risk of project failure.

The simplest scheme to implement from an I.T. perspective is the separate entitlement card model. The DVLA and Passport Agencies' cards and systems were developed to address specific requirements and are also constrained by international standards. The entitlement card is a different requirement; it is currently not constrained by international standards and will probably need different data and operating procedures from the Passport and DVLA cards. Allowing the project to focus on the specific objective of saving £650 million p.a. will result in the cheapest and fastest implementation. Following that implementation ways of interfacing the DVLA, Passport and Entitlement databases can be developed relatively cheaply.

Another factor that must be considered is the accuracy of the data held in the DVLA and Passport Office systems. For the Entitlement Card scheme to be successful in reducing fraud it is essential that the information held about the individual is accurate. A management view will be required as to whether the accuracy of the data held by the DVLA or Passport Agencies is sufficient in this context.

A further data source that could be considered (assuming it exists) is the data held by the Benefits Agency on current and past claimants. This is likely to have the most accuracy for the sector of the population where the risk of fraud is assumed to be greatest. However, this approach will obviously depend upon that data being available in a suitable format.

However, there may be a route to simplify the data capture phases of the project. Assuming that a separate database (the e-card database) is to be created then this could initially be loaded from the data currently held on the DVLA and Passport Agency databases. From a systems design perspective this procedure would be relatively trivial and, if designed correctly, would allow a manual data clean up exercise where the data on the Passport Agency and DVLA databases conflicted. This initial database load coupled with a data clean up exercise would mean that the e-card database would start life with some 35 million validated entries on it. This would vastly simplify the six year implementation period as only those citizens whose data was not held on the e-card database would now require validation. For those citizens whose data was already on the e-card database all that would be required is for their data to be updated if necessary when their entitlement card is issued.

Similarly, over the six year implementation phase of the entitlement card system a procedure should be considered whereby when an application for a new or updated Driving Licence or Passport is received an initial check is made to determine whether that citizen was already recorded on the e-card database. If the citizen is already recorded then the data held could be validated against the new information and corrections identified and sent to the e-card agency to allow the e-card database to be updated. If not then the relevant details could be sent to the e-card agency for addition to the database. This would ensure that an ongoing data synchronisation process was in place as early as possible and would reduce the scale of the inevitable data clean up exercise that would be required before automated synchronisation of the databases could be implemented.

P24 Page 48

Views are sought on whether young people should be invited to apply for an entitlement card when they are issued with a National Insurance Number.

As the proposal is to make this scheme universal the simplest option from an I.T. perspective is to automatically issue a card at a certain point. If it is decided that the appropriate point is when a National Insurance number is issued then the citizen should be given an appropriate appointment so that the relevant biometric data can be obtained and the card issued.

P25 Page 48

The Government is keen to hear young people's views on what features they would like to see on an entitlement card which would make it attractive to them.

The British Computer Society has no specific views on this other than to note that a frequent reason for failure in an I.T. project is the raising of expectations to a level that cannot be realistically delivered. This must be borne in mind when considering the responses to this point.

P26 Page 50

The Government invites comments on its suggestions for how entitlement cards could be issued to various categories of foreign nationals. The Government is particularly keen to ensure that any entitlement card scheme would not make the UK a less attractive place for foreign nationals to work and settle lawfully and welcomes specific suggestions on how to ensure this.

Clear identification of those agencies which would issue entitlement cards to non U.K. citizens would be required and the Entitlement Card Project Team could then design specific interface mechanisms to support each distinct procedure where an entitlement card could be issued. Priority would have to be given to those instances where a foreign national required a service from a government agency that would be dependent upon production of the entitlement card.

P27 Page 51

Views are invited on whether more background biographical checks than currently take place should be conducted before applicants were issued with entitlement cards and whether the checks suggested in this paper are useful, feasible and proportionate.

The British Computer Society has no comments to make on this point.

P28 Page 55

* **Comments are invited on whether an entitlement card scheme should include the recording of biometric information with particular regard to the cost, feasibility and acceptability of the three most likely options (fingerprints, iris patterns and facial recognition).**

* **The government would like to hear the views of potential partners on how a nation wide network of easily accessible biometric recording devices could be established and operated, how people who are not mobile or who live in sparsely populated areas could be served and what other value added services potential partners might offer.**

The British Computer Society can only respond to (i) above.

One of the commonest reasons for projects going significantly over budget, or even failing completely, is the over optimistic adoption of new technology. Two of the three biometric data possibilities being considered here depend very much on new technology.

AUTOMATED FACIAL RECOGNITION

The consultation paper does not identify if automated facial recognition has ever been implemented successfully anywhere and we are not aware of any successful implementation. However, one proposal in this consultation document is to use it as an identification mechanism on a database of 67.5 million entries.

In the commercial sector a risk of this magnitude to a project that is estimated to cost £1.3 billion (para 5.46, page 66) would never be contemplated.

Automated facial recognition must be evaluated very carefully in small non critical applications and systems. If it is proven to work successfully and accurately then the feasibility of scaling the process up to a database of 67.5 million entries must be tested comprehensively. If this testing proves successful then the possibility of implementing it for the entitlement card project may be considered.

IRIS SCANNING

The consultation paper admits that:

"... iris scanning has only been used to date on systems holding up to a few tens of thousands of records ... where there is a relatively fixed set of records against which to check and where an error by the system does not cause too much inconvenience." (page 107, para 38)

and also:

: "The banking industry believes that it will be 10 years before biometric checks will be used to validate day to day transactions." (page 125, para 83)

Spending some £1.3 billion to build a system that is dependent upon a database of 67.5 million iris pattern entries seems a trifle foolhardy in the light of these comments.

FINGERPRINTS

Of the three biometric possibilities being considered this is the most tried and tested mechanism for establishing an individual's identity.

Large-scale fingerprint processing applications do exist. However, this consultation paper gives no indication as to whether or not these applications have been reviewed to determine what sort of response times could be expected when comparing a fingerprint against a database holding (presumably) 10 times 67.5 million entries, i.e. 675 million entries.

The paper does discuss the options of off-line and on-line checking, but even in the off-line mode the average number of checks per day needs to be estimated to determine what the overall processing load will be.

In situations like this it is extremely easy to create a situation where the backlog is always increasing, as there is insufficient processing power available to process the requests for matches faster than they are requested.

PHOTOGRAPHS

Our view is that the use of photographs held on the card and in the central database would be the cheapest and most reliable way of establishing identification. The technology is available and has been used in many different applications for many years. It is a low risk approach that guarantees a high degree of security as a visual match between the photograph on the card and the photograph held on the central database would be sufficient for accurate identification of an individual in the vast majority of situations.

BIOMETRIC DATA COLLECTION

As well as the ongoing use of the biometric data discussed above the practicalities of the actual collection process must also be carefully considered.

In paragraph 16 on page 135 there is an estimate of 2,000 biometric recording devices being required should the decision be taken to use either iris pattern or fingerprint recognition.

Clearly there are numerous photograph facilities around the country should the decision be taken to use photographs.

It is not clear whether the estimate of 2,000 biometric recording devices would remain if automated facial recognition is chosen as the biometric identification mechanism.

As noted earlier the number of people who will be issued with an entitlement card is 67.5 million. The process of issuing these cards will occur over a 6 year period (table 5.3 on page 65). Assuming that there are 253 working days available in a year this equates to an average of approx. 44,500 people a day, or ca. 22 people per day at each biometric recording site over the 6 year period. This is an average of one person each 25 minutes.

The practicality of this must be tested. If the sites are mobile then the number of days they are available for is obviously reduced with a consequent impact on required throughput of people.

The mechanisms to be used to persuade people to attend on a regular basis need to be identified and tested. Will people be offered appointments or will they be expected to simply turn up? Either option carries with it significant management problems if the required throughput is to be achieved.

The impact that recording the biometric data could have on network traffic would also need to be considered carefully. The optimum solution would probably be to collect the data at the remote site during the day and then transfer it to the central computer(s) overnight. In this way the network traffic could be managed more easily.

The above arithmetic calculation assumes that no cards are re-issued over the six year period. As there will inevitably be lost and stolen cards the actual number of cards issued over the 6 year period could significantly exceed 67,500,000 giving another reason to review the proposed number of biometric recording devices.

The degree with which an individual's biometric iris, fingerprint pattern or facial structure physically degrades as they age may also need to be considered in terms of how frequently the data needs to be re-recorded.

If biometric information is recorded in the shape of iris, fingerprint patterns or facial structure then consideration also needs to be given to those situations in which the information needs to be checked to confirm identity. Performing an iris scan, taking a fingerprint or checking facial structure is a procedure that people may not tolerate if it occurs on a frequent basis. The length of time required to match the biometric data against what is recorded for the entitlement cardholder is also a non-trivial exercise and will not be an instantaneous process. Consideration of these practical difficulties associated with making use of the biometric data may lead to the decision that there is no point in recording it in the first place.

P29 Page 56

Views are sought on what benefits issuing an entitlement card as a smartcard would bring to card holders, whether the use of a smartcard chip could be shared by a number of organisations effectively and whether any potential partner would be interested in managing the sharing of a chip on behalf of the Government.

The primary issue with this proposal is the security aspects of various organisations sharing the data held on a single smart chip. If this is a specific requirement (note that there does not appear to be a specific business case identified for this requirement) then the most secure approach would be to hold the data on the central database rather than on the card itself. If it is to be held on the card then the problems that would need resolving include:

* Development of rigorous security controls to prevent unauthorised access of data on the smart card

* Development of routines to automatically update data held on the central database and on the card when the card data is changed. This will require close and ongoing liaison with those thirds parties granted access to data held on the smartcard chip.

The comments made on P4 are also relevant to this point as is the overriding concern that as this does not address the prime project objective of saving £650 million p.a. it should not be addressed until after that prime objective has been achieved. This is a classic example of 'scope creep'.

The issue of business continuity must also be addressed. Even if the project is restricted (correctly) to the prime stated objective of saving £650 million p.a. through a reduction in benefit fraud it must still be designed to cope with availability issues. A system like this has many points of failure and will have a set of very demanding users. If the system becomes unusable through one of the points of failure occurring then contingency plans must be available to ensure some level of service is maintained. The key points of failure are:

* Physical failure of the central processing computers

* Failure in the application software layer

* Failure in the proprietary operating and database management software ;layers

* Failure of the telecommunications network

* Failure of any of the above in the local site where the system is used in servicing the customers (people entitled to benefits)

P30 Page 60

Views are invited on the different ways which a card system could be used to help validate face to face, post, telephone and on-line transactions. In particular views are sought:

* **From service providers on whether an authentication service based on a card scheme would be useful.**
* **From potential partners who might provide the authentication service on a commercial basis to help off-set some of the costs of the scheme to the Government**
* **On the longer-term use of biometric information should this form part of any scheme.**

The British Computer Society has no comments to make on this point.

P31 Page 60

Views are invited on whether it would be feasible in business and technical terms for an entitlement card to include a digital certificate and what the implications for the cost of the card would be.

As the cards are not going to be used for any commercial transactions there is no obvious reason as to why a digital certificate is required to protect the legal owner of the card.

The only situation where a digital certificate would currently be relevant is in controlling the production of forged cards. However, the biggest safeguard against this would probably be through the use of encryption techniques rather than digital certificates.

If digital certificates are used than scalability issues must be considered as the signing authority would need a validation capability sufficiently powerful to handle a large number of transactions per day.

P32 Page 62

Views are welcomed on what information should be held in any central register which might be used to administer a card scheme and what information should be displayed or stored on the card.

Given the volatility of address information consideration should be given to not displaying an address on the card. Most (if not all) commercial credit/debit cards do not display this information on the card but do use it as a secondary validation check.

There is no clear reason for storing the biometric data on the card. One obvious issue is where the readers will be situated should this data need to be read from the card. Holding this data on the central database will allow authorised third party service providers to access it for necessary validation without the need for dedicated reading devices.

One option that should be seriously considered is that a Central Register should be maintained of all cards issued which contains only the information held on the card and a quite separate database used by the Entitlement Card Administration Authority (ECAA).

There are several advantages in this approach. The Central Register could be available on-line to all authorised users: Social Security Offices, Housing Benefit Offices, etc: A person presenting a card does not have to be asked for permission to access the Central Register since it can only be accessed for the purpose of validating the information on the card and for visual confirmation that the person presenting the card is indeed the person concerned (the digital photo transmitted back would be likely to be larger and clearer than that on the card). No other information is available than that already provided by the person presenting the card.

The ECAA Database would not be available on-line to these agencies. It can thus hold information that for some people is sensitive without any threat (real or apparent) to that person's privacy (address, former name, etc).

With this approach one can get some clarity into the discussion of what information is held where and what are the rules of access and by whom. There can also be a technical audit to ensure that it is not possible to obtain unauthorized access to the information in the ECAA Database.

P33 Page 63

The Government is very keen to consider suggestions from people whose circumstances might make it difficult for them to participate in a scheme and from organisations representing them on how a scheme can be designed to accommodate their needs.

COMMMENT REQUIRED FROM THE DISABILITY SG??

P34 Page 68

Comments are invited on the indicative costs outlined in this section, in particular on the compliance costs which employers might incur in using a card to check the employment status of new employees.

This consultation paper does not define the scope to be provided by the I.T. system. In fact there are several suggestions that would change the final scope substantially if they were adopted. It is, therefore, difficult to review the costs in any accurate way.

If the assumption is made that the project objective is to save £650 million p.a. by reducing entitlement fraud and that all of the other possibilities discussed are outside the scope of this project and therefore outside of the estimated costs then some comments can be made.

SET UP COSTS

IT Central Register and links to other systems - cost £107 million

The rationale behind this figure is highly subjective and more detailed analysis is required before any realistic cost can be calculated. In particular the number of links to other systems is highly ambitious for such a complex project (paragraph 12 page 134). These should be reviewed carefully and a phased approach taken to drastically reduce the risks currently associated with this project.

Biometric recording equipment - cost £29 million for 2000 items, i.e. £14,500 each

This is an estimate based upon a risk assessment. Proper estimates are required from reputable suppliers to obtain a firm estimate on this.

OPERATING COSTS

Operating costs for smartcards

These are obviously simply dependent upon supplier quotations once the level of required sophistication is decided.

The costs have been estimated based upon an assumption that smart cards will last on average 5 years. This seems to be higher than currently experienced by commercial providers of smart card schemes and it is possible that costs should be re-estimated based on a shorter elapsed time, say 3 or 4 years. This will obviously have an impact on costs in two ways - the cost of the cards themselves as well as the administrative costs associated with issuing more cards p.a.

IT Central Register and links to other systems - cost £263 million p.a.

Biometric recording equipment - cost £69 million p.a.

Whilst these figures seem high as a result of the arbitrary inclusion of amounts to reflect the perceived 'high risk' of I.T. projects there is no detailed analysis available to contradict it.

Additional staff - cost £62 million over 13 years

Processing Applications - cost £608 million (appears to be 'one off' not p.a.)

It is not really possible to comment on these costs unless more detailed assumptions are made available.

Card Production

The costs here are obviously dependent upon the decisions made as to the degree of sophistication of the card and the subsequent supplier quotations.

COST RECOVERY

As previously noted the central objective of this scheme appears to be the saving of £650 million p.a. in fraudulent claims in the public sector. The User Project Management should be charged with achieving this saving thus removing any need for cost recovery as the system becomes self-financing. This will result in more effective project management and greatly increase the chances of success for this project.

OTHER COST CONSIDERATIONS

The other cost factor to take into account is the lifetime of the project and the fact that the technologies being employed will change over that time scale.

This will need very careful management to avoid unnecessary cost. There is an inevitable human tendency to associate new technology with new functionality and to have an expectation of immediate delivery of the benefits from that new technology. If, for example, encryption techniques are changed during the project implementation period of 6 years (which they inevitably will) then a management issue will obviously be whether or not to re-issue all of the cards already in circulation to the new encryption standard because of perceived incremental savings.

Other similar issues that are likely to arise are

* Changes in the capability of smartcard chip recording and reading devices (both bio-metric and non bio-metric)
* Changes in chip technology on the smart cards
* Changes in Database Management Software, Operating Systems and Computer Programming Languages
* Changes in infrastructure standards, leading to such issues as backwards compatibility of functionality
* Etc.

The project budget should include an amount to allow essential technology change to be incorporated into the project plan. Having the correct management judgement to correctly decide what is essential in this context is mandatory if major cost escalations and timetable overruns are to be minimised.

P35 Page 75

Views are invited on what specific measures should be included in any entitlement card scheme to ensure compatibility with the principles of the Data Protection Act 1998.

The scheme has to be consistent with the Data Protection Act 1998, Directive 95/46/EC, the Human Rights Act 1988 and the Council of Europe Convention on Human Rights and Fundamental Freedoms.

Nigerian (and other) Scams

Many of you may have received emails requesting your help in moving (dubious) funds from Nigeria to another country. These are known as 419 scams in relation to the section of the Nigerian penal code that seeks to stamp out this sort of thing. Some of these letters are highly amusing and I reproduce some of those that I have received during the last six months after the report below. - Ed.

Edward Venning, spokesman for the UK's The National Criminal Intelligence Service said: "For the past 18 months we have been receiving around 1,000 emails per week reporting these scams and we are constantly working to collate the intelligence from these emails. "From the intelligence we have gathered from victims of this fraud we were able last year to secure 24 arrests and convictions in South Africa and 12 in the UK." Furthermore, according to Venning, the UK is one of only two countries in the world dealing with this problem so proactively, with the other being the US through the Secret Service. To put the problem into perspective, last year alone 150 people were victims of this fraud, according to NCIS figures. The average amount of money lost by these victims was £56,675 - a figure boosted by the fact that a couple of victims were already millionaires before being tempted by the fraudulent 'get-rich-quick scheme'. While many of these victims will find sympathy hard to come by, Venning countered the suggestion that these scams are undeserving of lengthy, and costly investigation, explaining that the problem is far more serious than a few fools being easily parted from their money. According to Venning, the unwitting individuals who hand over their bank details to these scammers are directly funding the trafficking of Class A drugs into Europe from Africa as well as other activities such as car crime. And Venning believes there is still much more which needs to be done - starting with the ISPs, the main conduit nowadays for 419 correspondence. He said: "ISPs in general are adopting a 'head in the sand' attitude towards this problem."

However, the victims in all this aren't only those who are receiving the emails. It's likely the close association with fraud has irreparably damaged the reputation of Nigeria. "From a business perspective this scam reflects very badly upon Nigeria as a country," said Venning, adding that the Nigerian High Commission has worked very closely with NCIS to crackdown on the handful of individuals whose actions have tarnished the country's image. The problem is now moving further away from its roots in Nigeria as a result of the notoriety this scam has achieved. According to Venning, Nigeria has now used up its "trust capital" - meaning it is now so inextricably linked with fraud that emails from within the country are almost always regarded with suspicion. As such many of the fraudsters are decamping to South Africa.

Here are some examples received by the editor.

PETROLEUM (SPECIAL) TRUST FUND

LAGOS-NIGERIA

CONFIDENTIAL

REQUEST FOR URGENT BUSINESS PROPOSAL

From the Desk of: Dr. Fahd A.Usman.

Dear Sir,

This letter may come to you as a surprise since it is coming from someone you have not met before. However, we decided to contact you based on a satisfactory information we had about you.

I am a Medical Doctor currently working with the Petroleum Trust Fund (PTF). I and some of my close and trusted colleagues need your assistance in the transfer of US$21.8 million into any reliable Account you may nominate overseas.

This fund was generated from over-invoicing of contracts executed by the PTF under our control and supervision. This fund is now ready to be remitted into any Account we put forward for that purpose. What we want from you is a good and reliable company or personal Account into which we shall transfer this fund. Details should include the following:

1. Name of Company, Address & Your Private Telephone & Fax Number.

2. Name of Bank & Address of Bank .

3. Account Number

4. Beneficiary Name

Upon receipt of your company & bank particulars, an application shall be made in your name to the Central Bank of Nigeria for the approval of the remittance of the funds which shall be by SWIFT (Telegraphic transfer) copies of the approval and other relevant documents shall be faxed to you for your perusal.please treat as strictly confidential for obvious reasons. The fund will be shared as follows:

1. 17% for your assistance

2. 80% for myself & my Colleagues

3. 3% for contingency expenses

We wish to assure you that your involvement should you decide to assist us, will be well protected, and also, this business, proposal is 100% risk free as the remittance will be made through the legal procedures. Note: your discussions regarding this transaction should be limited because we are still in government service. We intend to retire peacefully at the end of this transaction. Let honesty and trust be our watchword throughout this transaction and your prompt reply will be highly appreciated.

Thank you for your anticipated cooperation while we look forward to a mutually benefiting business relationship with you. Best Regards.

Dr. Fahd A.Usman.

234 1 7754093 phone.

234 1 7599055 fax

FROM: RANDY LAWANI

Dear Sir,

REQUEST FOR A BUSINESS RELATIONSHIP.

This letter may come to you as a surprise but it was out of my sincere desire to share a mutual business relationship with you. I got to know of you through an international directory forwarded to me by the family of late President Kabila of The Democratic Republic of Congo, in which your designation and status as a capable Godly personality who can be trusted. Hence

I deem it fit to confide in you.

I am a solicitor by name Randy Lawani, a personal lawyer to the Kabila family and consequently represent their interest with due respect to their monetary affairs. The family has $9.000.000:00[nine Million United States Dollars] currently in a security company vault; this huge sum of money is in a coded form. The present President Joseph Kabila intends to use this money for investment purposes without the consent of any foreign body outside the family.

To come straight to the point, this money has been moved from Congo through Switzerland to Amsterdam in The Netherlands, and the Kabilas need you as a reliable investor that could be trusted with the PIN and CERTIFICATE OF DEPOSIT to enable us use the funds outside The Democratic Republic of Congo. After lots of deliberations and considerations I as the family lawyer with the authority invested in me to immediately work on ways and means of transferring this sum of money to a reliable and trust worthy foreign partner that will be able to help and assist us secure the funds in a suitable account. I am convinced you are the right person to handle the said proposal, if we have to achieve our goals and objective.

Moreover, the personal identification Number Certificate Deposit and The Letter of Authority from my law firm that will facilitate transfer of the funds is in my possession. Since no name was used in securing the funds in the vault, your name will be passed and tagged on the consignment of funds as the rightful owner.

The family have reached an agreement with me that 25% of the total sum of the funds will be for your assistance towards this transaction. 5% for eventual expenses that might be incurred on the course of this transaction if any, and 70% will be invested by you in other business of interest for the family.

Finally, I wish to assure you that this transaction will not attract any risk on your behalf. Furthermore, all documentations covering this transactions will be sent to you for Verification.Your response is urgently required in other to speed up the process.

Thanks in advance.
Randy Lawani,
Esq, [Barrister]

DR.FRANK.F.BAMAWO
FOREIGN LIAISON OFFICE
NIGERIA NATIONAL PETROLEUM CORPORATION (NNPC)
AMSTERDAM, THE NETHERLANDS.
URGENT BUSINESS PROPOSAL.

Dear Sir/Madam,

I am an accountant with the Nigeria National Petroleum Corporation (NNPC) and, also a member of the Contract Review committee. Presently, I'm on a special diplomatic duty in the Nigeria foreign office in Amsterdam,the Netherlands. A contract for the construction and laying of oil pipelines network from Warri-Port-Harcourt-Kaduna.has been awarded to a local firm and, this contract was over invoiced to the tune of Nine Million, Six Hundred Thousand United State Dollars (US$9. 6Million).

The over invoicing was a deal by my committee to benefit from the project, and now the local contractor have been fully paid but, the over invoiced amount is still floating in one of the offshore banks of Central Bank of Nigeria in Canada .We now desire to transfer this money which is presently in a suspense account of the Central Bank of Nigeria (CBN) into any overseas account which we expect you to provide for us, if you are capable and able.

For providing, the account where we shall remit the money,you will be entitled to 20% of the money,70% will be for myself and my partners,the remaining 10% will be set aside to settle all expenses incurred by both parties.

I would require the following;

1.Bank name and Address

2.Name of Beneficiary

3 Company Name and Address

4. Account Number.

5. Confidential Telephone and Fax number of Beneficiary.

The above information would be used to make formal applications to the appropriate government parastatals such as the Federal Ministry of Finance (FMF), Nigerian National Petroleum Corporation (NNPC) and the Central Bank of Nigeria (CBN) as a matter of procedure for the release of the money and onward transfer to the nominated account you would provide. In as much as , we are doing a deal, we would like to comply with all laid down procedures for transfer and contract of this nature. It does not matter whether or not your company did this contract or not. The assumption is that your company was awarded the major contract and subcontracted it out to the local company. We have strong and reliable connections and contacts at the Apex Bank and the Federal Ministry of Finance All we need is a trust worthy foreign partner to assist us in this mutual/beneficial deal.

Therefore, when the business is successfully concluded,we shall through our same connections withdraw all documents used from all the concerned Government Ministries for 100%security.We are civil servants and we do not want this opportunity to miss us, as opportunity loss can never be regained

Please contact me immediately through my e-mail address,whether or not you are interested in this deal. If you are not,it will enable me scout for another foreign partner to carry out this deal.But where you are interested, send the required document aforementioned herein without delay,as time is of great essence in this deal.

I await your anticipated co-operation and response.
Best Regards
DR.FRANK BAMAWO.

Dear Sir/Madam,

I am Mr.Chetamma John, the Manager accounting & auditing department of the Eagle Bank of Nigeria Ltd at 31/37 Toyin street Ikeja. Lagos, it is with utmost trust and confidence that I make this urgent and important business proposal to you. I want your assistance and co-operation in carrying out this business opportunity in my department. I discovered an abandoned sum of $22.200.000.00 (Twenty two million two hundred thousand united state dollars) in a fixed deposit account that belongs to one of our foreign customers who died in 1997 in a plane crash,(flight details : Korean airlines, Boeing 747-300, # hl-7468). He was into oil contracts with federal government before his death.

Unfortunately, none of his Asian family has come for the money, which I honestly believe they did not know about, neither the family members nor the relations has appeared to claim the money. Upon this discovery, I and the assistant manager of my department has now decided to seek for a foreigner who will stand as a relation of the dead client. We have ideas as bankers how we can get the money to you with out any trouble.

We are willing to offer to you an agreeable percentage. We are absolutely positive that this deal will be of mutual benefit to us and also create room for future business relationship.

We expect you to treat this with utmost confidentiality, trust and sincerity.

Thanking you for your anticipated co-operation.

Reply to: johncheta@caramail.com

Yours Faithfully.

Chetamma John.

FROM:Berry Marvelous.

PHONE:(874)-762864167,

FAX :(874)-762864168,

(URGENT AND CONFIDENTIAL)

RE: TRANSFER OF ($26,000.000.00 USD}

TWENTY SIX MILLION DOLLARS

Dear Sir,

We want to transfer to overseas account ($26,000.000.00 USD) Twenty six million United States Dollars) from a Prime Bank here in South Africa, I want to ask you, If you are not capable to quietly look for a reliable and honest person who will be capable and fit to provide either an existing bank account or to set up a new Bank a/c immediately to receive this money, even an empty a/c can serve to receive this money, as long as you will remain honest to me till the end for this important business trusting in you and believing in God that you will never let me down either now or in future.

I am Mr.Berry Marvelous, the Auditor General of one of the prime banks here in South Africa, during the course of our auditing,I discovered a floating fund in an account opened in the bank in 1996 and since 1998 nobody has operated on this account again,after going through some old files in the records I discovered that the owner of the account died without a [Heir/WILL] hence the money is floating and if I do not remit this money out urgently it will be forfeited for nothing. The owner of this account is PEDRO F. HASLER a foreigner, a great industrialist and he died since 1998.No other person knows about this account or any thing concerning it, the account has no other beneficiary and my investigation proved to me as well that until his death he was the manager GOLD ARK [pty]. SA.

We will start the first transfer with Six million [$6,000.000] upon successful transaction without any disappoint from your side, we shall re-apply for the payment of the remaining rest amount to your account.

The total amount involve is Twenty six million United States Dollars only [$26,000.000.00]. I want to first transfer $6,000.000.00 [Six million United States Dollar] from this money into a safe foreigners account abroad before the rest. But I don't know any foreigner, I am only contacting you as a foreigner because this money can not be approved to a local person here, without valid international foreign passport, but can only be approved to any foreigner with valid international passport or drivers license and foreign a/c because the money is in US dollars and the former owner of the a/c is a foreigner too, and the money can only be approved into a foreign a/c.

However, we will sign a binding agreement, to bind us together when we meet face to face after the first transfer of $6 Million before transferring the second part of $20 Million. I am revealing this to you with believe in God that you will never let me down in this business, you are the first and the only person that I am contacting for this business, so please reply urgently so that I will inform you the next step to take urgently. Send also your private telephone and fax number including the full details of the account to be used for the deposit.

I want us to meet face to face to build confidence and to sign a binding agreement that will bind us together immediately after the first transfer before we fly to your country for withdrawal, sharing and investments.

I need your full co-operation to make this work fine because the management is ready to approve this payment to any foreigner who has correct information of this account, which I will give to you upon your positive response and once I am convinced that you are capable and will meet up with instruction of a key bank official who is deeply involved with me in this business. I need your strong assurance that you will never, never let me down.

With my influence and my position in the bank the bank official can transfer this money to any foreigner's reliable account that you can provide with assurance that this money will be intact pending our physical arrival in your country for sharing. The bank official Will destroy all documents of transaction immediately we receive this money leaving no trace to any place and to build confidence you can call me for heart to heart discussion through my private satellite phone which I secured for the security and safety of this business as you know that this business is confidential. I will use my position and influence to obtain all legal approvals for onward transfer of this money to your account with appropriate clearance from the relevant ministries and foreign exchange departments.

At the conclusion of this business, you will be given 35% of the total amount, 60% will be for me, while 5% will be for expenses both parties might have incurred during the process of transferring. I look forward to your earliest reply through my email address.

Yours truly,

Berry Marvelous

DONATION FOR THE LORD

From: Mrs. Sarah Rowland

PLEASE ENDEAVOUR TO USE IT FOR THE CHILDREN OF GOD.

I am the above named person from Malaysia. I am married to Dr. Alan George Rowland who worked with Malaysia embassy in South Africa for nine years before he died in the year 2000. We were married for eleven years without a child. He died after a brief illness that lasted for only four days. Before his death we were both born again Christians. Since his death I decided not to re-marry or get a child outside my matrimonial home which the Bible is against. When my late husband was alive he deposited the sum of $27.6Million (twenty-seven Million six hundred thousand U.S. Dollars) with one West-Falia finance/security company in London United Kingdom. Presently, this money is still with the Security Company. Recently, my Doctor told me that I would not last for the next three months due to cancer problem. Though what disturbs me most is my stroke. Having known my condition I decided to donate this fund to church or better still a christian individual that will utilise this money the way I am going to instruct here in. I want a church or individual that will use this to fund churches, orphanages and widows propagating the word of God and to ensure that the house of God is maintained. The Bible made us to understand that Blessed is the hand that giveth. I took this decision because I don't have any child that will inherit this money and my husband relatives are not Christians and I don't want my husband's hard earned money to be misused by unbelievers. I don't want a situation where this money will be used in an ungodly manner, hence the reason for taking this bold decision. I am not afraid of death hence I know where I am going. I know that I am going to be in the bossom of the Lord. Exodus 14 VS 14 says that the lord will fight my case and I shall hold my peace. I don't need any telephone communication in this regard because of my health, and because of the presence of my husband's relatives around me always. I don't want them to know about this development. With God all things are possible. As soon as I receive your reply I shall give you the contact of the West-Falia Finance/Security Company in United Kingdom. I will also issue you a letter of authority that will empower you as the original- beneficiary of this fund. I want you and the church to always pray for me because the lord is my shephard (sic). My happiness is that I lived a life of a worthy Christian. Whoever that wants to serve the Lord must serve him in spirit and truth. Please always be prayerful all through your life. Any delay in your reply will give me room in sourcing for a church or christian (sic) individual for this same purpose. Please assure me that you will act accordingly as I stated herein. Hoping to hear from you.

Remain blessed in the name of the Lord.

Yours in Christ,

Mrs Sarah Rowland.

BCS IRMA SPECIALIST GROUP ADVERTISING RATES (Apr 03)

Reach the top professionals in the field of EDP Audit, Control and Security by advertising in the BCS IRMA SG Journal. Our advertising policy allows advertising for any security and control related products, service or jobs.

For more information, contact John Mitchell on 01707 851454, fax 01707 851455 email john@lhscontrol.com.

There are three ways of advertising with the BCS IRMA Specialist Group:

The Journal is the Group's award winning quarterly magazine with a very defined target audience of 350 information systems audit, risk management and security professionals.

Display Advertisements (Monochrome Only) Rates:

- Inside Front Cover £400
- Inside Back Cover £400
- Full Page £350 (£375 for right facing page)
- Half page £200 (£225 for right facing page)
- Quarter Page £125 (£150 for right facing page)
- Layout & artwork charged @ £30 per hour

Inserts can be included with the Journal for varying advertising purposes, for example: job vacancies, new products, software.

Insertion Rates:

For inserts weighing less than 60grams a flat fee of £300 will be charged. Weight in excess of this will incur additional charges:

• 60-100grams:	14p per insert
• 101-150g:	25p per insert
• 151-300g:	60p per insert
• 301-400g	85p per insert
• 401-500	105p per insert

Thus for an insert weighing 250g it would cost the standard £300 plus weight supplement of £210 (350 x 60pence) totalling £510.

Discounts:

Orders for Insert distribution in four or more consecutive editions of the Journal, if accompanied by advance payment, will attract a 25% discount on quoted prices.

Direct mailing

We can undertake direct mailing to our members on your behalf at any time outside our normal distribution timetable as a 'special mailing'. Items for distribution MUST be received at the office at least 5 WORKING DAYS before the distribution is required. Prices are based upon an access charge to our members plus a handling charge.

Access Charge £350. Please note photocopies will be charged at 21p per A4 side.

Personalised letters:

We can provide a service to personalise letters sent to our members on your behalf. This service can only be provided for standard A4 letters, (i.e. we cannot personalise calendars, pens etc.). The headed stationery that you wish us to use must be received at the Office at least ten working days before the distribution is required. Please confirm quantities with our advertising manager before dispatch. If you require this service please add £315 to the Direct mailing rates quoted above.

Discounts: Orders for six or more direct mailings will attract a discount of 25% on the quoted rates if accompanied by advance payment

Contacts

Administration

Janet Cardell-Williams,
49 Grangewood, Potters Bar, Hertfordshire EN6 1SL
Email: janet@carliam.co.uk
Website : www.bcs-irma.org

BCS IRMA Specialist Group Advertising Manager

Eva Nash Tel: 01707 852384 & 07973 532358
E-mail : eva@nash141.freeserve.co.uk

HUMOUR PAGE

Some new words to enliven your audit reports

BLAMESTORMING: Sitting around in a group, discussing why a deadline wasmissed or a project failed, and who was responsible.

SEAGULL MANAGER: A manager who flies in, makes a lot of noise, craps on everything, and then leaves.

ASSMOSIS: The process by which some people seem to absorb success and advancement by kissing up to the boss rather than working hard.

SALMON DAY: The experience of spending entire day swimming upstream only to get screwed and die in the end.

CUBE FARM: An office filled with cubicles.

PRAIRIE DOGGING: When someone yells or drops something loudly in a cube farm, and people's heads pop up over the walls to see what's going on.

MOUSE POTATO: The on-line, wired generation's answer to the couch potato.

STRESS PUPPY: A person who seems to thrive on being stressed out and whiny.

XEROX SUBSIDY: Euphemism for swiping free photocopies from one's workplace.

PERCUSSIVE MAINTENANCE: The fine art of whacking the hell out of an electronic device to get it to work again.

ADMINISPHERE: The rarefied organisational layers beginning just above the rank and file. Decisions that fall from the adminisphere are often profoundly inappropriate or irrelevant to the problems they were designed to solve.

404: Someone who's clueless. From the World Wide Web error message "404 Not Found", meaning that the requested document could not be located.

OHNOSECOND: That minuscule fraction of time in which you realise that you've just made a BIG mistake.

Some useful phrases for your next audit report

It has long been known — I didn't look up the original reference.

A definite trend is evident — This data is practically meaningless.

Three of the samples were chosen for detailed study — The others didn't make any sense.

Typical results are shown — This is the prettiest graph.

These results will be in a subsequent report — I might get around to this sometime, if pushed/funded.

In my experience — Once.

In case after case — Twice.

In a series of cases — Thrice.

It is believed that — I think.

It is generally believed that — A couple of others think so, too.

Correct within an order of magnitude — Wrong.

A careful analysis of obtainable data — Three pages of notes were obliterated when I knocked over a glass of vodka

It is clear that much additional work will be required before a complete understanding of this phenomenon occurs — I don't understand it.

After further study by colleagues — They don't understand it, either.

Thanks are due to Joe Blotz for assistance with the experiment and to Cindy Adams for valuable discussions — Mr Botz did the work and Ms Adams explained to me what it meant.

A highly significant area for exploratory study — A useless topic selected by my committee.

It is hoped that this study will stimulate further investigation in this field — I quit.

DOES THIS REMIND YOU OF YOUR COMPANY?

Once upon a time the government had a vast scrap yard in the middle of a desert. Parliament said, "someone may steal from it at night." So they created a night watchman position and hired a person for the job.

Then Parliament said, "How does the watchman do his job without instruction?" So they created a planning department and hired two people, one person to write the instructions, and one person to do time studies.

Then Parliament said, "How will we know the night watchman is doing the tasks correctly?" So they created a Quality Control department and hired two people. One to do the studies and one to write the reports.

Then Parliament said, "How are these people going to get paid?" So they created the following positions, a time keeper, and a payroll officer, then hired two people.

Then Parliament said, "Who will be accountable for all of these people?" So they created an administrative section and hired three people, an Administrative Officer, Assistant Administrative Officer, and a Legal Secretary.

Then Parliament said, "We have had this in operation for one year and we are £1,800,000 over budget, we must cut back overall cost."

So they laid off the night watchman.

IRMA

INFORMATION RISK MANAGEMENT & AUDIT

◆ A SPECIALIST GROUP OF THE BCS ◆

BCS

THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	John Bevan	Audit & Computer Security Services	01992 582439 john_bevan@ntlworld.com
DEPUTY CHAIRMAN	Pete Biss	EMX Co Ltd	01279 858300 pete_biss@hotmail.com
SECRETARY	Siobhan Tracey	BFG plc	01494 442883 siobhan.tracey@booker.co.uk
TREASURER	Jan Lubbe	KPMG	020 7774 8303 Jan.Lubbe@gs.com
MEMBERSHIP SECRETARY	Celeste Rush		020 8858 7384 RushLSE97@aol.com
JOURNAL EDITOR	John Mitchell	LHS Business Control	01707 851454 john@lhscontrol.com
WEBMASTER	Allan Boardman	Goldman Sachs	07881 930814 webmaster@bcs-irma.org
SECURITY PANEL LIAISON	John Mitchell	LHS Business Control	01707 851454 john@lhscontrol.com
MEMBER SERVICES BOARD LIAISON	Celeste Rush		020 8858 7384 RushLSE97@aol.com
EVENTS	Siobhan Tracey	BFG plc	01494 442883 siobhan.tracey@booker.co.uk
	Alex Brewer	Lloyds TSB	020 7418 3544 alex_brewer@bigfoot.com
	Rosemary Mulley	NabarroNathanson	0118 950 5640 r.mulley@nabarro.com
ACADEMIC RELATIONS	David Chadwick	Greenwich University	020 8331 8509 d.r.chadwick@greenwich.ac.uk
LOCAL GOVERNMENT LIAISON	Peter Murray		01992 582105 cass@peterm.demon.co.uk

Membership Enquiries to:

Janet Cardell-Williams
49 Grangewood, Potters Bar, Herts EN6 1SL
t: 01707 852384
f: 01707 646275
e: members.irma@bcs.org.uk
www.bcs-irma.org

IRMA

INFORMATION RISK MANAGEMENT & AUDIT

◆ A SPECIALIST GROUP OF THE BCS ◆

BCS

THE BRITISH COMPUTER SOCIETY

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) * * Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal *(see over)*	£75
INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)*	£25
INDIVIDUAL MEMBERSHIP *(A members of the BCS)* BCS membership number: _______________________	£15
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)

E-mail:

PROFESSIONAL CATEGORY: (Please circle)
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify)

SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS IRMA"AND RETURN WITH THIS FORM TO

Janet Cardell-Williams, IRMA Administrator, 49 Grangewood, Potters Bar, Herts EN6 1SL. Fax: 01707 646275

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

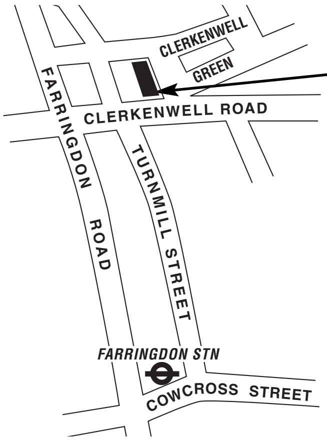
E-mail:

PROFESSIONAL CATEGORY:
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify)

Venue for

Full Day Briefings

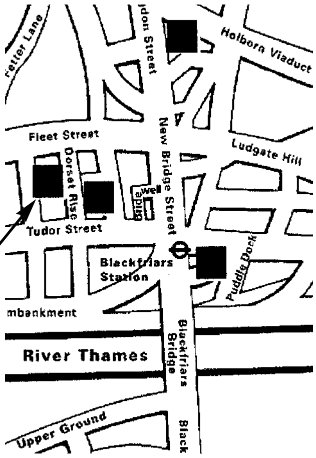
(except 4 November 2002)



Old Sessions House
Clerkenwell Green
London EC1

Venue for

Late Afternoon Meetings



KPMG
8 Salisbury Square
London EC4