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

JOURNAL
volume 15 number 1 spring 2005 ISSN 1741-4229

40th ANNIVERSARY YEAR, 1965-2005

Programme for members' meetings 2004 – 2005

Tuesday 7 September 2004 Late afternoon	**Computer Audit Basics 2: Auditing the Infrastructure and Operations**	16:00 for 16:30 KPMG
Thursday 7 October 2004 Full day	**Regulatory issues affecting IT in the Financial Industry**	10:00 to 16:00 Old Sessions House
Tuesday 16 November 2004 Full day	**Networks Attacks – quantifying and dealing with future threats**	10:00 to 16:00 Chartered Accountants Hall
Tuesday 18 January 2005 Late afternoon	**Database Security**	16:00 for 16:30 BCS
Tuesday 15 March 2005 Full day	**IT Governance**	10:00 to 16:00 BCS – The Davidson Building, 5 Southampton Street, London WC2 7HA
Tuesday 17 May 2005 Late afternoon AGM precedes the meeting	**Computer Audit Basics 3: CAATS** ***Preceded by IRMA AGM***	16:00 for 16:30 BCS – The Davidson Building, 5 Southampton Street, London WC2 7HA

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 map see back cover.

Contents of the Journal

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 be by e-mail and 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 electronic digital image.

Submission Deadlines

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

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

It's hard to believe that it was as long ago as 1965 that some far sighted individuals created the Auditing by Computer (ABC) specialist group of the BCS. Now, forty years on, the Information Risk Management and Audit (IRMA) specialist group is its direct descendant. During that time there have only been a handful of chairmen; Ron Middleton, William List, myself, Alison Webb, John Bevan and currently Alex Brewer. We are the oldest, continuous specialist group in the Society and as we enter our ruby anniversary I believe it not unreasonable to reflect on the changes that have taken place since the Group's formation.

Mainframe computers ruled the roost for the first twenty years. Slowly developing from a single program capability to multi-tasking leviathans. The very first computer that I can remember was an Elliot 808 with paper tape input. I was introduced to it on a school visit to London University in the mid 1960s. I played tic-tac-toe (a kind of noughts and crosses game) against it and lost. In those days you were required to have two Advanced levels, one of which had to be in mathematics to even operate a computer! My first work machine was a CDC 3200. The 3200 reflected its memory of 32k bits. It had eight tape drives which used 2,400 feet reel to reel serial tapes, an 80 column punched card reader, a line printer which used continuous paper and a teletype for operator-to-machine communication. Initial Program Load (IPL) "booted" the operating system so that the single application could be loaded. This was the machine on which I cut my operating and programming (COBOL) teeth. An eight-tape sort in a darkened room was a sight to behold. The flashing lights on the tape drives, coupled with the whirring of the reels were the stuff of science fiction and I was part of it!

During the early 1970s I graduated to a CDC 6400 (twice the memory), then through the IBM 360 and 370 ranges, Univac's 1100 series and onto Honeywells and ICLs. The early ICL machines (1902s, 1903s and 1904s) used the George 2 operating system, but then ICL developed VME/B which was built with security in mind from the ground up. I remember that the VME/B High Security Option received an unprecedented B1 security rating from the American Department of Defence, at a time when security was a cumbersome bolt on extra for the IBM MVS operating system. I generated and implemented a CICS teleprocessing system and got to grips with network protocols, dumb terminals and fixed drum storage and exchangeable hard disks. I audited hierarchical databases, such as IMS-X and made a small name for myself by writing an audit programme to guide other auditors through the torturous process of gaining assurance that it was well controlled. I used Filetab and Easytrieve for my interrogations and found some amazing things, such as the £9 billion asset, the £6 parcel of land and incorrect depreciation and age of debt calculations. I was edging my way onto the international conference circuit by flying the then novel idea of looking at the data to identify control deficiences rather than using the resource intensive system based audit approach. I applied the second law of thermo dynamics to data integrity and found that it worked quite well.

Meanwhile, mid-range machines in the form of PDPs and VAXs were coming through, but I couldn't take them seriously until the IBM Series 3 and later the IBM 400 came on the scene. Then in the late 1970s the dawn of the microcomputers, in the form of Commodores, Apricots and Superbrains (really), which used the CP/M (Control Program for Micro-processors) operating system, heralded the move to what we have now. The dominant operating system became MS-DOS which transformed into the Windows we know today. During that time I moved away from COBOL and into relational databases such as dB2, which gave me a grounding in Oracle and the visual languages. However, what I leaned in my mainframe education stood me in good stead for what we have today and will have tomorrow.

This Group grew with along with the technology and at its largest we had well over 500 members, but we lacked, and still do so, an essential requirement of a professional body; a qualification. This has left us vulnerable to other professional bodies, such as ISACA, which offers its CISA and CISM qualifications.

During my 25 years with the Group I have met some marvellous people who have moved computer auditing from an art form to a science. We drank more alcohol in those days (it was socially acceptable) and so did the IT crowd. If you wanted information, then the interviewing technique involved taking the systems programmer to the local pub and drinking him/her under the table. The technique may be questionable, but it still beats the hell out of flowcharting the system! I find that today's computer auditors take themselves far to seriously, but then we tend to be better qualified now than the IT people. We have

MIIA, CISA, QiCA, CISM and CISSP to mention just a few and most computer audit jobs require one of these, whereas the IT lot are mostly professionally unqualified (for example, only a small percentage are members of the BCS). This really should give us an edge, but I still see computer auditors on the defensive when dealing with the techno gabble of the IT people and I still see SLAs written from the point of view of the supplier rather than the customer. My red pen comes out as I try to turn these into business speak and to identify the associated metrics. IT governance is primarily about measurement. "If you can't measure it, you can't manage it", is my motto, but determining the relevant metrics is not easy. I am reminded of what John F Kennedy, the young President of the USA in the 1960s said. "We do these things not because they are easy, but because they are hard". Easy measurements tend to be useless from a governance viewpoint. After all, how do you measure the value added of IT to the business? Well, I have a few solutions, but commercial confidentiality prevents me from sharing them with you. After all, I have to eat too!

However, reading this journal can help you to move closer to solving that problem. Vasilis Katos from Portsmouth University provides an insight into how you can apply mathematical techniques to obtain optimum network configuration. Jack Vivret discusses the implications of the Freedom of Information Act and Bob Ashton describes the Australian approach to dealing with trans-national high tech crime. Mark Smith details the benefits he has negotiated for you and Colin Thompson updates us on the activities of our parent body. Happy reading.

John Mitchell

PLEASE NOTE THE EMAIL ADDRESS FOR

IRMA ADMIN

IS:

admin@bcs-irma.org

Chairman's Corner

Where's my data gone?

Do you know with any certainty where all of your important data has gone? Let's keep it simple and just try to track the important stuff. If you can answer this question with any certainty, then some of the following may apply:

- You are very precise and know where everything in your business has gone, including the data,
- Your business is quite small, and the number of computer users is less then two!
- You haven't really thought about it at all...

I have written a pop quiz below for you to see if you know where your data is.

The Big Question

If I were to ask for the list of your organsation's critical data assets, would you have one to hand (even if a bit out of date)?

Outsourced?

If you have outsourced anything to a large company, then they will very likely outsource parts of it across the globe: perhaps your data has made it as far as Glasgow, Manila, or Hyderabad. But did you know it had got there, and did you know how well it is protected?

'Borrowed'?

Perhaps it's outsourced to a service company who tend the servers, run the backups. Perhaps your organisation or the service company outsource their cleaning to a company that specialise in that sort of thing. In the case of both companies, was any security clearance obtained? If not, perhaps the data has been 'borrowed'? It would not be obvious if a backup tape were copied, and might not be visible if it were removed...

Transferred?

Perhaps you transfer your data via the internet to one of a number of 'data vault' backup sites? In which case, the internet address of the company might be the same as the country that they are resident, but using the concept of 'virtual domains' it could be anywhere.

Given away?

One of the most embarrassing reports I saw was where some enterprising students bought old hard disks from second hand shops and internet auction sites and found personal data on most of them (credit card numbers by the thousand, medical records etc). Indeed, identity thieves have themselves worked out that this is a good way to get people's personal data without having to raid their home or wade through their dustbins, if they can find their old computer.

So where is it?

One of the properties overlooked about data is that it is invisible. Resident on a disk, in transit on a network, lodged in memory it is always invisible. You cannot see it without the help of computers, which turn it into something you can see, but you need to know it is there first. So unless you know where to look, you might overlook some important piece of vitally important data. So where is your data?

Alex Brewer

Where is my data - pop quiz:

Yes; give yourself 3 points,
Maybe; give yourself 2 points,
No; give yourself 1 point.

1. ( ) There are complete records of all PCs decommissioned so that the items can be retraced if necessary.
2. ( ) The organisation knows where its backup tapes are stored, how many copies should be there and how long they are kept before they are destroyed.
3. ( ) The organisation's Internet Service Provider does not outsource any part of their business.
4. ( ) The organisation's web servers are hosted and located in the EU.
5. ( ) The critical servers used by the organisation are all maintained in house, OR The organisation has received security clearance for all people working on its servers and applications resident on them.
6. ( ) The out of hours and subcontract staff working on site have been security cleared.
7. ( ) The organisation has a list of all its critical data assets.
8. ( ) All hard disks and PCs removed from the organisation are cleansed of all data before they are released.
9. ( ) USB 'key drives', CD burners and floppy disks are banned from the organisation.
10. ( ) The organisation's data is protected by encryption when in transit to the outsource site.

Total points ( ).

- If you got more than 20 points, you are doing well - time to consider the weakest links remaining.
- If you got from 11-20 points, perhaps it's time to look at the big picture and consider what the organisation can and cannot afford to lose.
- If you got 10 or less, you are probably being honest!

The Down Under Column

Bob Ashton – IRMA Oceania Correspondent

Transnational High Tech Crime

The Australian Institute of Criminology has recently published a paper titled "Impediments to the Successful Investigation of Transnational High Tech Crime", authored by Dr. Russell G. Smith. Seven barriers to the effective investigation of high tech crime across borders are identified, and some solutions are offered that could be used to streamline future investigations in this area.

The following is an abstract of the paper:

Suspect Identification

Digital technologies enable people to disguise their identity in a wide range of ways making it difficult to know for certain who was using the terminal from which an illegal communication came.

Online technologies make it relatively simple to disguise one's true identity, or to make use of someone else's identity.

Even e-commerce technologies that make use of public infrastructures and digital signatures can be easily manipulated by individuals presenting fabricated documents to support a false identity when obtaining a key pair from a registration authority for use in secure transactions.

It has been found that those internet services that provide the highest levels of anonymity are most likely to be used for criminal purposes.

Response Strategy

Advanced technologies of user authentication and verification with issuing authorities.

Criminal law and extradition

Where an accused person is resident in a country other than the one in which criminal proceedings are to be taken, it is possible for that person to be extradited to stand trial. However, the procedures involved in extradition are complex and difficult, making applications costly and slow.

Response Strategy

Implementation of treaties and harmonisation of high tech crime laws.

Choice of jurisdiction

Where offences are omitted in various countries, or where the offender and victim are located in different places, questions arise as to which court should deal with the matter.

Response Strategy

United Nations protocol on the determination of jurisdiction in cross-border criminal cases.

Search and seizure

Difficult problems arise in obtaining digital evidence in high tech crime cases, although in some ways computers have made the process easier through the ability to conduct searches of hard drives remotely via the internet.

Often transnational high tech crime operations need to be closely coordinated. Warrants may need to be simultaneously executed in different countries in order to ensure that suspects do not collaborate in their alteration or destruction of evidence.

Response Strategy

Legislative reform of powers of search and seizure and targeted use of warrants.

Encryption of Evidence

A difficult problem facing high tech crime investigators concerns data that have been encrypted by accused persons who refuse to provide the decryption key or passwords.

Response Strategy

Legislative reform to compel disclosure of keys and allow police to undertake covert key recovery activities.

Mutual assistance

The central difficulty is the slow and cumbersome nature of official requests.

Response Strategy

Streamlining mutual assistance procedures, increasing resources to agencies to respond to requests, and delegating requests to branch offices of organizations.

Logistical and practical problems

Conducting investigations across national borders raises many practical problems that delay matters and increase costs.

Response Strategy

Enhanced international cooperation and increased funding to expedite investigations.

For further information: www.aic.gov.au

Statistical Risk Cluster Analysis for Network Segmentation[1]

Vasilios Katos
Department of Information Systems and Computer Applications,
University of Portsmouth, Portsmouth
email: vasilios.katos@port.ac.uk

Abstract

This paper describes a method to determine the number of network segments - tiers - in a network which is hosting a number of applications with different security requirements. The method requires input from a risk assessment process where the applications are grouped on selected criteria and produces an overall grouping of applications using statistical clustering methodologies. The method can be used as a tool for assisting the network segmentation decision process, and is particularly useful for application migration from a "closed" system to an e-business platform, since the latter typically includes applications with considerable differences in their security requirements.

Keywords

network segmentation, risk analysis, security profile, cluster analysis

1. Introduction

There exists a wide range of documentation dealing with network segmentation (often referred to as compartmentalisation) for security purposes, [1], [2]. Today the most popular component for implementing network segmentation is the firewall [3]-[5], which is typically employed to shield a corporate network perimeter from a high risk untrusted network, for example the Internet [6], [7]. However, other network components such as routers and switches can also be configured to perform network segmentation, not only for efficiency but also for security sake. In fact, many routers are embedded with firewall software in order to perform advanced segmentation and filtering [8]. A significant amount of work has been published concerning the technical details of performing network segmentation, by developing security policies for the firewalls [9] and assigning access lists, traffic monitoring and control on the different layers [10], [11].

Segmentation is also performed within the private corporate network. Although the main reasons involve efficiency and manageability, many organizations – such as banking and military - require classified network areas with different access levels. In general, there is a plethora of reasons organizations decide to segment their network. For example, organizations who have employed a "closed" Information System to implement their business processes for some years and have decided to use a public network like the Internet in order to improve their processes, face a considerable number of challenges, one of which is security. More specifically, the security requirements of an application existing in an "open" system [12] which leverages the established internetworking standards, are quite different from those requirements of a "closed" and more controlled system [13].

[1] A preliminary version of this paper appeared in INC 2004 – Fourth International Network Conference, Plymouth, 6-9 July 2004.

Due to the diversity of applications, their security requirements may vary and in some cases may cover the whole security spectrum ranging from low security applications (e.g. publicly available yellow pages), to very high security levels (e.g. applications which handle trade secrets like formulas for medicine, soft drink recipes, as well as air traffic information). Ideally, each application with its specific set of security requirements would have an infrastructure designed, implemented and operated in a way to meet those security requirements. In practice however, this is economically infeasible, when the number of applications is high. In addition, many organizations decide to outsource hosting [14], for cost effectiveness. Outsourcing leverages a third party's existing infrastructure and experience thus lowering the risks for human error. In addition, the speed of implementation is higher.

Once it is realized that every application cannot have a dedicated infrastructure, the system owner is then requested to decide on the grouping of applications in a way that applications with "similar" security requirements can be placed together in a common infrastructure which meets those security requirements. In addition, the total number of distinct infrastructures (differentiated on a security requirement basis) must be selected. The whole process may be seen as a breakeven analysis, were the cost parameters refer to the cost of the infrastructure investment, and the cost of a security breach. The cost of the infrastructure investment includes the cost of the security investment where parts of this cost are present in the costs of design, implementation, testing, operation and maintenance.

The purpose of this paper is to provide a method for identifying the expected number of network segments, from a risk perspective. In reality there are many technical and organisational factors which influence the actual network segmentation; the goal of this methodology is to merely advise on the number of segments based on the outcome of a risk analysis process.

2. The process framework

Let n be the number of network segments. Our task is to determine a suitable n based on the security requirements of the applications hosted by a network infrastructure.

1. The process consists of four main steps:
2. The risk assessment
3. The informal risk classification
4. The security profile generation and classification
5. The cluster analysis-based grouping

The success of the proposed method is heavily dependent on the efficiency of the risk assessment process. A number of risk assessment methodologies can be found in the literature, see for example [15]. It is accepted that risk assessment methodologies have inherent limitations, as the assessment data involved can be incomplete, biased or inappropriate. Consequently, the proposed method is bound by the success factor of the underlying risk assessment.

The proposed method requires two main inputs from the risk assessment. The first input is the application risk placement on the risk plane. This information will be used for the informal risk classification (step 2). The second input required is the application ranking according to predetermined risk classification criteria. In the proposed method three risk classification criteria are used, namely confidentiality, integrity and availability; most risk assessment processes operate in the context of these three criteria. This information will be used for the security profile generation (step 3).

The estimation of the lower bound of the number of groups *n* is an informal risk classification process. The output of this process is a risk classification map which is a diagram and its purpose is to provide graphically a rough idea of the risk distribution of the applications. The graphical representation of the risk classification is later used as a sanity check, by comparing the output of the formal classification performed at a later stage with the early results of this stage. Sanity checks are vital when performing automated tasks, because automation focuses on time efficiency rather than accuracy.

2.1. The informal risk classification

The informal risk classification is presented in Figures 1 and 2. This approach employs two fundamental elements; the probability of an event occurring and the likely loss should it occur. The vertical axis represents the cost (or damage) of a threat being successful, whereas the horizontal axis represents the likeliness of security breach. All applications are placed on the risk plane, as shown in Figure 1 for an example of 27 applications. The "annual loss expectancy", or the "estimated annual cost", which is calculated for any event by simply multiplying the potential loss by the corresponding probability, ranks events in order of risk, as shown in Figure 2. It should be noted that the cost axis could represent any type of a loss metric forming an ordered set. For instance, some organisations may use a set such as {negligible, minor damage, major damage, catastrophic} to describe losses. For each element in the set a numerical value is assigned and this value would represent the cost.

An "iso-risk curve" is a classification boundary which has the characteristic that all points belonging to the curve represent the same risk. An iso-risk curve close to the point (0,0) represents a lower risk than an iso-risk curve which is further from (0,0). From the infinite iso-risk curves, we may select those that do not intersect the areas with high application densities. As a result, the iso-risk curves separate the areas with similar risk levels and consequently the applications are grouped according to risk. In the example in Figure 2 we may identify two iso-risk curves and therefore the risk plane is segmented into three distinct regions, indicating thus a number of groups n=3. Generally, if b represents the number of the iso-risk curves selected, the lower bound of n would then be b+1.

In the same example applications 26 and 27 are in the same group and have high risk. However, the risk can be high due to the different levels of the classification criteria. For instance, application 26 may have a high risk due to confidentiality, whereas the risk of application 27 may be high due to availability. An example functionality of application 26 can be a business logic handling medical data. An example functionality of application 27 can be an SMS gateway where guaranteed delivery is required. Consequently, although two or more applications are grouped together in the same risk level, the respective risk values can be originated from different classification criteria and therefore further segmentation and grouping may be required.

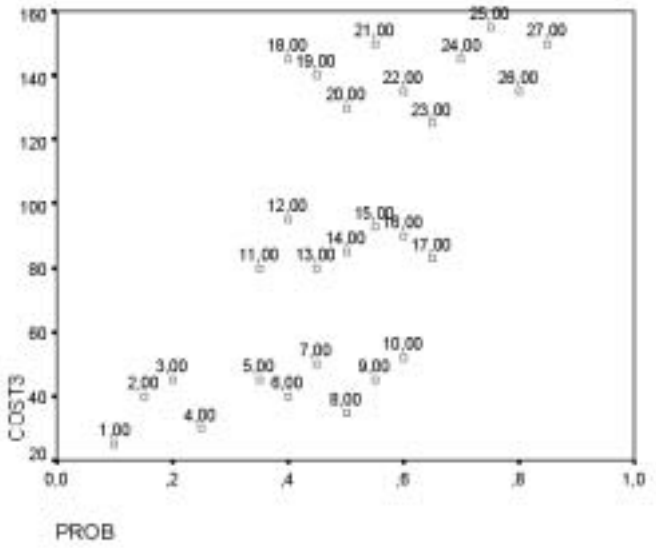

Figure 1 Application placement

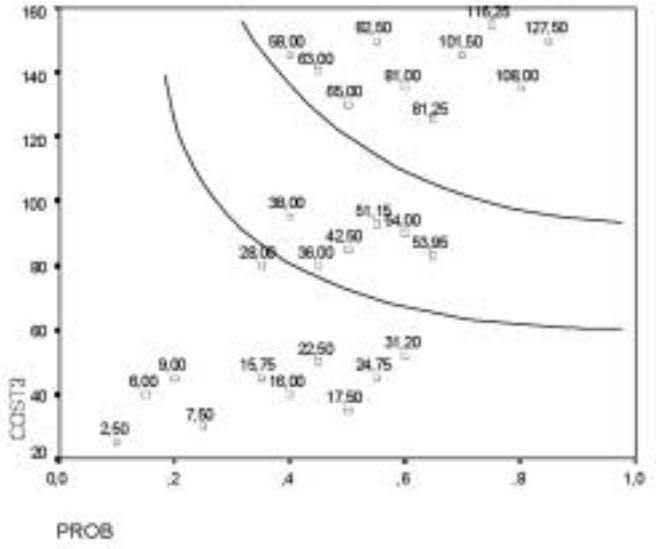

Figure 2 Risk classification

2.2. Generation of the security profile

The security profile refers to assigning values to the classification criteria for each of the applications. These values can have a numerical form (such as "1,2,3,…") or a descriptive form (such as "high, med, low, very low,…"). It should be highlighted that the values are distinct, finite and form an ordered set. Let l be the cardinality of this set, which represents the number of distinct values a classification criterion may have. Then, if c is the number of classification criteria, the upper bound of n (or granularity) would be c^l. Typically c is usually equal to three (representing confidentiality, integrity and availability) and l is also equal to three. In this paper $l=3$ and the classification values used will be "H,M,L", representing a "High", "Medium" and "Low" value. Summarizing for n the following holds:

$$b+1 \le n \le c^l$$

The process of generating the security profile must be the same for all applications. Once more, drawing from the risk assessment process, the levels of confidentiality, integrity and availability are obtained for every application or functionality group of the system. The result is normalized to the three values of "H" "M" and "L" for each classification criterion and the security profile of the application is generated. The form of the

security profile could be expressed as follows:

<application_name>[confidentiality,integrity,availability].

For example, an application handling yellow pages information could have the following security profile:

yellow_pages[L,M,M]

Continuing on the example of Figure 1 and assuming that c=3 (confidentiality, integrity, availability) and l=3 (L,M,H), each application may have one of the $c^l = 3^3 = 27$ security profiles. In the example we assumed that we are considering 27 applications in order to attach, for generality, each different security profile to each application. In our example, however, the attachment of the security profile to applications is rather arbitrary. The security profiles of all applications of the example are shown in Figure 3. To each application (point in Figure 3) five data variables are attached: cost, probability, confidentiality, integrity, availability.

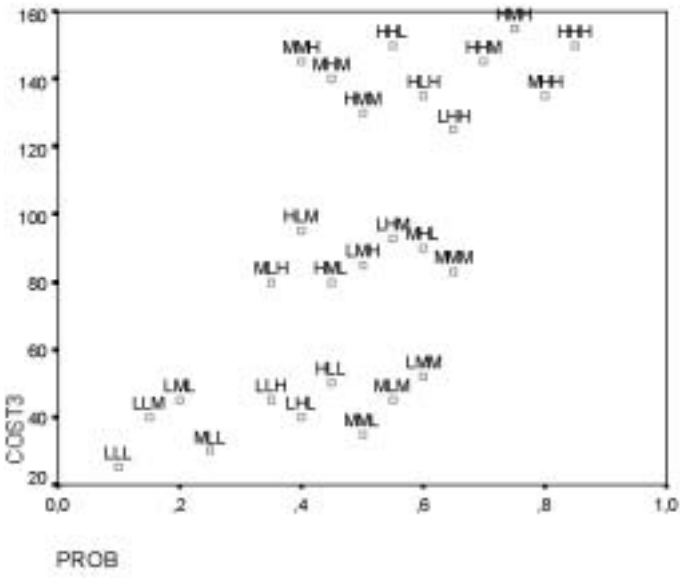

Figure 3 Security profiles of applications

2.3. The grouping framework

As stated earlier, the purpose of the security classification process is to group applications with similar security requirements in order to pursue a cost effective and efficient implementation. For this grouping the statistical methodology of cluster analysis may be employed. Cluster analysis classifies a set of observations into two or more mutually exclusive unknown groups based on combinations of variables. The purpose of cluster analysis is to discover a system of organizing observations into groups where members of the groups share properties in common [16], [17].

Clusters identified by the analysis are typically based on two properties: internal cohesion and external isolation. Internal cohesion implies that items within the same cluster are similar to one another. External isolation implies that the items in one cluster are separated from the items in another cluster by some form of an empty space. The differences among the various algorithms used in cluster analysis are primarily due to the metrics that are used for calculating similarities between items and for combining items into clusters [18]. The following two clustering procedures may generally be distinguished [19], [20]:

- Hierarchical clustering: According to this procedure, clustering begins by finding the closest pair of items according to a distance measure and combines them to form a cluster. The procedure continues one step at a time, joining pairs of items, pairs of clusters, or an item with a cluster, until the data are in one cluster. This procedure involves the construction of tree-like structures called dendrograms for identifying the clusters. A dendrogram that clearly differentiates groups of items will have small distances in the far branches of the tree and large differences in the near branches.
- K-means clustering: According to this procedure, clustering begins by using the values of the first k items in the data file as temporary estimates of the k cluster means, where number k is specified by the user. Initial cluster centres are formed by assigning each item in turn to the cluster with the closest centre and by updating these centres the process continues until no further changes occur in the centres. This procedure involves an ANOVA methodology for identifying variables that drive the clustering.

For both, hierarchical clustering and K-means clustering, the following points are important:

- Standardization method: The results of the clustering methods depend on the values of the variables involved. Therefore, the variables must be initially transformed on the same scale. Usual transformations include “z-scores” and “0 to 1 scale”.
- Distance measure: The procedures use dissimilarities or distances between items when forming clusters. The “squared Euclidean distance”, which is the sum of the squared distances over all variables, is used most frequently.
- Linking method: The procedures use amalgamation rules to determine when two clusters are sufficiently similar to be linked together. Two commonly used methods for combining clusters are the “between groups method”, which uses the concept of the nearest distance neighbour in joining clusters, and the “Ward’s method”, which uses an analysis of variance approach to evaluate the distances between clusters.

Using the five variables of the risk assessment procedure and the security profile of applications presented in the example of Figure 3, we will present below the results of the hierarchical clustering and the K-means clustering grouping methods of the 27 applications (items or cases) in the example. For both grouping methods the variables involved have been transformed into a “0 to 1 scale”, the distance measure is the “squared Euclidean distance” and the linking method is the “Ward’s method”. For all estimations the SPSS 11.0 statistical package has been used.

2.3.1. Results employing hierarchical clustering

According to this method the number of clusters is initially unknown. The dendrogram obtained in Figure 4 will help us to identify the number of clusters. From the rescaled into 0 to 25 distance cluster combine we see that the dendrogram clearly differentiates groups of items that have small distances in the far branches of the tree and large differences in the near branches. We may say that this dendrogram clearly indicates three clusters, as shown by the three intersections of the bold line drawn at the 12.5 level of scale with the large branches of the tree.

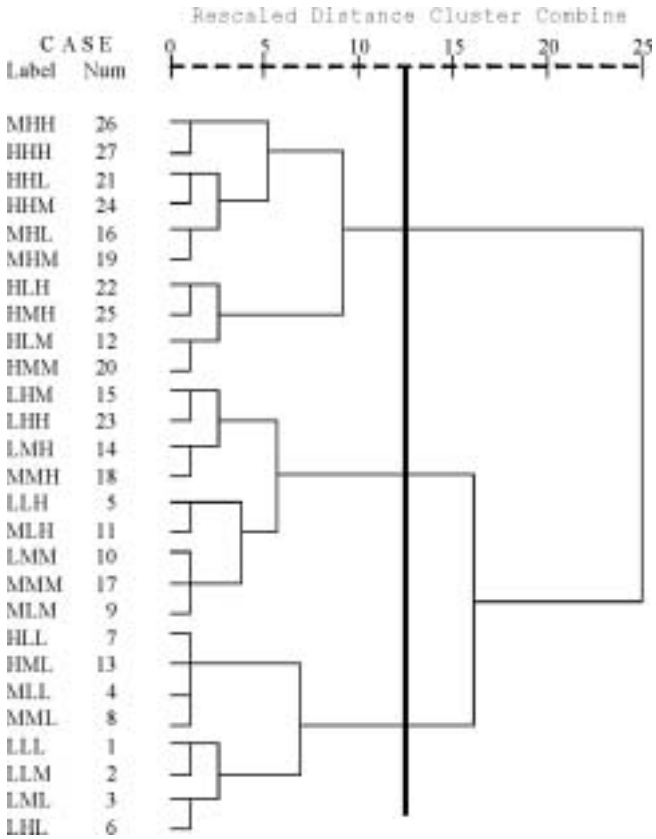

Figure 4 Dendrogram using Ward's Method

Although the specific applications that belong in each cluster are shown in the dendrogram, Figure 5 indicates the groups where the applications belong. Comparing the grouping of applications in Figure 2 with the grouping of applications in Figure 5 we may see some differences. For example, applications 18 and 23 are assumed to be high risk applications when we only use the risk assessment data in Figure 2, and medium risk applications when we combine in the hierarchical clustering method the risk assessment data and security profile data in Figure 5.

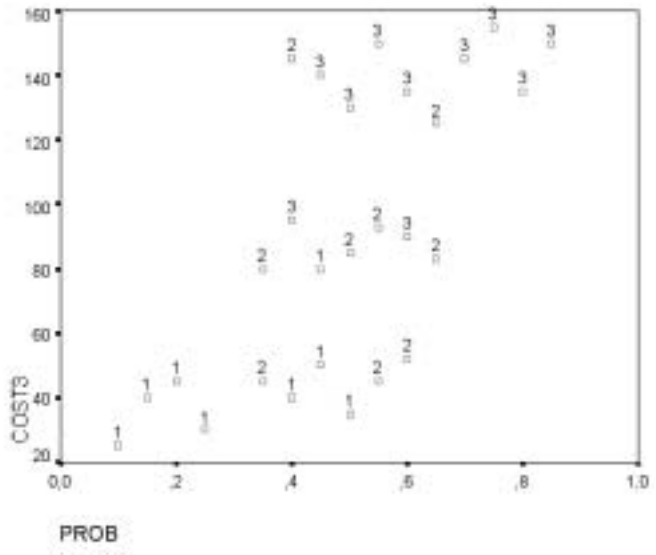

Figure 5 Grouping of applications using hierarchical clustering

2.3.2. Results employing K-means clustering

According to this method the number of clusters is initially known. In our case we assume that this number is equal to three, obtained either in the informal risk assessment in Figure 2, or in the hierarchical clustering in Figure 5. However, this number of clusters may be verified by the ANOVA procedure that this clustering methodology is employing. In Table 1 we see that the contribution of each variable in the clustering is statistically significant at a 0.05 significant level, as it is shown by the significances of the F statistic. Thus, we may accept that our initial number of clusters is correct.

Table 1 ANOVA from the K-means clustering

Variables	Cluster Mean Square	Degrees of Freedom	Error Mean Square	Degrees of Freedom	F	Sig.
Cost	1,238	2	2,536E-02	24	48,805	,000
Probability	,264	2	4,565E-02	24	5,789	,009
Confidentiality	1,342	2	7,567E-02	24	17,736	,000
Integrity	,703	2	,129	24	5,455	,011
Availability	,509	2	,145	24	3,505	,046

Figure 6 indicates the groups where the applications belong according to the K-means clustering. Comparing the grouping of applications in Figure 6 with the grouping of applications in Figure 5 we may see some differences. For example, applications 18 and 23 are assumed to be high risk applications when we only use the risk assessment data in Figure 2, or when we combine in the K-means clustering method the risk assessment data and security profile data in Figure 6, and medium risk applications when we combine in the hierarchical clustering method the risk assessment data and security profile data in Figure 5. Thus, we see that the high risk group contains the same applications when we use the informal risk assessment method and the K-means clustering method.

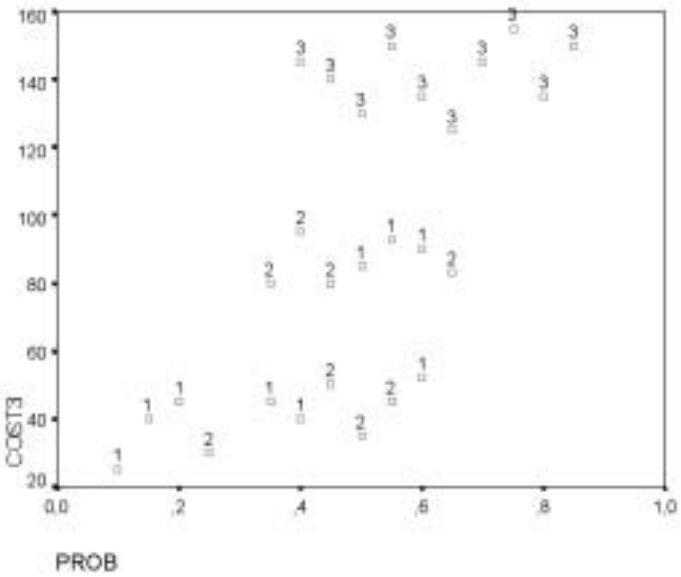

Figure 6 Grouping of applications using K-means clustering

In more detail, Table 2 presents the similarities and the differences in the grouping of applications according to the hierarchical clustering and the K-means clustering methodologies. Although there are differences in the specific applications belonging in each group, overall, we see that 9 vs. 8 applications, 8 vs. 9 applications and 10 vs. 10 applications belong in the first, second and third group respectively, according to the hierarchical clustering vs. the K-means clustering.

Table 2 Hierarchical versus K-means clustering (number of applications)

		K-means Method			Total
	Groups	1	2	3	
Hierarchical	1	4	4	0	8
Method	2	4	3	2	9
	3	1	1	8	10
Total		9	8	10	27

However, the two clustering methods show a very high association in similarly grouping applications, considering the significant values of the $\chi^2(4)=13.576$ [prob=0.009], the Pearson's R = 0.594 [prob=0.001] and the Spearman Correlation Coefficient = 0.605 [prob=0.001], which may be derived from the data in Table 2 [21].

3. Conclusions and Future Directions

The method described in this paper can be used when evaluating the network infrastructure in conjunction with the hosted applications. The purpose of the method is to assist to the selection of the number of network tiers or segments in order to balance costs with business risk by using selected risk classification criteria. Usually these criteria are confidentiality, integrity and authentication, but the method allows selection of an arbitrary set of criteria, since they are involved in the risk classification process, which in turn can be an arbitrary process itself. However, the classification success highly depends on the selection of the risk classification process and in addition the output of the process must be normalized to the selected set of classification criteria.

Having presented above that the results of the proposed method depend on the risk assessment reports, on the generation of the security profiles of the applications, and on the statistical clustering approaches followed, more work is needed to propose a more robust methodology. However, although the cluster analysis methodology is rather efficient, it is not a cookbook for effective grouping of applications and therefore it should be used carefully. Although in the proposed method, the risk assessment and the generation of security profile of applications were considered prerequisites for the cluster analysis followed, this may not be always the case. The cluster analysis may be applied directly to all variables describing the applications. However, if the two prerequisites are needed, we advise the interested researcher to use the "factor analysis" methodology in order to reduce the large number of initial variables into a smaller number (e.g. five in our example) of easily interpretable variables.

References

[1] R. Rusli, Secure System Architecture and Design, SANS GIAC Security Essentials, Dec. 2001.

[2] Rekhter, Y., B. Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear. Address Allocation for Private Internets, RFC 1918, 1996.

[3] C.Chapman, D. Brent, E. Zwicky. Building Internet Firewalls, O'Reilly and Associates, Inc., 1995.

[4] M. Ranum. Thinking About Firewalls, SANS-II Conference Proceedings, April 1993.

[5] C. Brenton, Firewalls 101: Perimeter Defense with Firewalls, SANS Security Conference Proceedings, Washington, D.C.: July 2000.

[6] NIST. Connecting to the Internet: Security Considerations, CSL Bulletin, National Institute of Standards and Technology, July 1993.

[7] F. Avolio and M. Ranum. A Network Perimeter With Secure Internet Access., Internet Society Symposium on Network and Distributed System Security, pp.109-119. Internet Society, February 2-4 1994.

[8] CISCO, Network Security Policy: Best Practices White Paper, http://www.cisco.com/warp/public/126/secpol.html, 2002.

[9] S. Hambridge, C. Smothers, T. Oace, J. Sedayao, Just Type Make! Managing Internet Firewalls Using Make and Other Publicly Available Utilities, USENIX Proceedings, First Conference on Network Administration April 7-10, Santa Clara, California, 1999.

[10] B. Fraser (ed.), Site Security Handbook, RFC 2196, 1997.

[11] R. Oppliger, Internet Security: Firewalls and Beyond, Communications of the ACM, Vol 40. No. 5, 1997.

[12] NIST. Security in Open Systems, NIST Special Publication 800-7, 1994.

[13] A. Anton and J. Earp, Strategies for Developing Policies and Requirements for Secure Electronic Commerce Systems, Recent Advances in Secure and Private E-Commerce, Kluwer Academic Publishers, 2001.

[14] J. Toigo, The Essential Guide to Application Service Providers, Prentice Hall, 2002.

[15] G. Stoneburner, A. Goguen, A. Feringa, Risk Management Guide for Information Technology Systems, NIST, Special Publication 800-30.

[16] M.S. Alderfer and R.K. Blashfield, Cluster analysis, Beverly Hills, C.A., Sage Publications, Inc, 1986.

[17] D.W. Stockburger, Multivariate Statistics: Concepts, Models, and Applications, http://www.psychstat.smsu.edu/multibook/mlt04m.html. Accessed 14/12/2004.

[18] M.L. Toms, M.A. Cummings-Hill, D.G. Curry and S.M. Cone, Using Cluster Analysis for Deriving Menu Structures for Automotive Mobile Multimedia Applications, SAE 2001 World Congress, Detroit, Michigan, March 5-8, 2001.

[19] STATISTICA, Electronic Textbook, StatSoft, Inc., http://www.statsoftinc.com /textbook/stcluan.html.

[20] SPSS, SPSS Base 11.0, Applications Guide.

[21] M.L. Berenson and D.M. Levine, Basic Business Statistics, Concepts and Applications, Englewood Cliffs, N.J., Prentice-Hall, 1992.

Preparing for Freedom of Information in the UK

Jack Vivrett

Introduction

A great deal of confusion still seems to exist regarding the compliance expectations being placed on UK public organizations due to the Freedom of Information Act (FOIA), which took effect in January 2005. Even though a lot of information is available about the FOIA, many organizations affected by the act have yet to make a serious move to develop and implement the records-management and information-transparency procedures required by FOIA, let alone integrate any new technology that will support these FOIA compliance activities. Much of the confusion seems to be focused on not knowing exactly how specific FOIA statutes manifest themselves into the actual actions that relevant bodies need to take in order to ensure FOIA compliance.

Given the level of information available and the confusion surrounding it, the purpose of this article is not to explain all of the various minutiae of the FOIA; rather it attempts to inform the reader about the key themes of the act, the types of general activities information-holding organizations will need to engage in order to comply with key features of the Act, and the types of technology tools these organizations should consider implementing in order to support their FOIA compliance activities.

FOIA overview

The United Kingdom's comprehensive Freedom of Information Act (FOIA), which took effect in January 2005, formalises the concepts of information transparency and accessibility. Under the basic terms of FOIA, any member of the public will be able to apply for access to information held by bodies across the public sector: affected parties include groups such as Parliament, national and local government bodies, health trusts, doctors' surgeries, publicly funded museums and thousands more. To support this initiative, the FOIA provides a detailed framework of rights for UK citizens who request information, as well as the adherence obligations for the majority of government, public and professional bodies covered under the Act. In addition, the FOIA establishes a broad enforcement structure to make sure its core requirements are followed in consistent and effective fashion.

The Act itself is long and detailed, which makes comprehensive understanding of it a real challenge for both affected organisations and the broader public. However, many resources have been made available to clarify all or parts of the act; of particular note is the website set up by the UK's Department of Constitutional Affairs (DCA) [http://www.dca.gov.uk/foi/index.htm] to address FOIA issues.

One part of the DCA website is dedicated to providing an overview of the key components of the Act, information that can prove invaluable to groups needing some idea about the most important areas to address when developing their compliance programmes. According to this site, FOIA features of particular importance are:

- "a general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions;
- in most cases where information is exempted from disclosure there is a duty on public authorities to disclose where, in the view of the public authority, the public interest in disclosure outweighs the public interest in maintaining the exemption in question;
- a new office of Information Commissioner…, and a new Information Tribunal, with wide powers to enforce the rights created
- a duty imposed on public authorities to adopt a scheme for the publication of information. The schemes, which must be approved by the Commissioner, will specify the classes of information the authority intends to publish, the manner of publication and whether the information is available to the public free of charge or on payment of a fee."

The level of complexity involved in each FOIA element, however, can prove particularly frustrating for organisations that are committed to creating compliant procedures and acting upon them accordingly. In other words, understanding the Act is one thing, but being able to fully understand its implications for specific organisations and how these implications can be dealt with is another thing altogether.

Impact of the FOIA on organisational activities

Depending on the government body, actual compliance schemes need to have been submitted to the government by the end of 2003 (in some cases, such as the police and prosecuting bodies, the deadline was end-of-June 2003) with full compliance in place by January 2005. Given the reach and impact of the FOIA, one could assume that many organisations in the UK would have had their compliance procedures and supporting activities in place, or nearly in place, by January 2005 deadline. However, many organisations do not. To a large extent, this inactivity is not necessarily based on complacence or ignorance of the FOIA. Rather, it is because the connection between FOIA policy and how it translates into actual organisational procedures remains murky for many affected public bodies. These organisations are reluctant to commit resources to the implementation of solutions that they are not sure will satisfy the FOIA requirements. These organisations have made it their explicit strategy to "wait out" the deadline in the hopes that as repercussions for non-compliance actually start playing out, more clarity about how best to meet FOIA expectations will come to light, thereby helping to focus organisational decision making.

Realising that this approach has a lot of inherent risk in it, many organisations are calling on area experts to advise them about the best course of action for pre-empting, or at least minimising, any serious ramifications caused by not meeting FOIA-related activities. One of these experts is Cinzia Biondi, a leading UK specialist in technology and information law and a senior associate in the Finance, Projects and Technology group

of Wragge & Co LLP. Due to her extensive knowledge in the area, one of Ms. Biondi's primary roles is providing FOIA-focused consultancy services for clients in the public and private sector.

According to Ms. Biondi, "The Freedom of Information Act will affect every area within the public sector, from health care to local government authorities in England and Wales. Parts of the public sector are either ignoring or panicking about the pending cut-off date, so clearly there is still a growing need for informative but practical material on the Act to help guide the public sector in the measures which can be taken to avoid a crisis. Although it is difficult to foresee the full impact of this change, most organisations will be telling staff they should assume all e-mails, paper and electronic documents that they write and receive will be discloseable."

Ms. Biondi continues, "In the commercial world, the Act is a huge issue for anyone sending information to a public body, as it may be accessed by the public at large and by anyone in the world, whether that is a lobby group, campaigner, competitor or journalist. The risk is that information which private sector organisations want to keep confidential, perhaps even that which provides competitive advantage in the marketplace, may get disclosed. This means that disclosure issues will affect contractual arrangements which the private sector enter into with the public sector and will influence changes in tendering processes and information sharing under public contracts including, PPP and PFI deals. Part of the strain within the public sector is financial. Compliance with associated legislation such as the Data Protection Act and initiatives such as meeting the eGovernment agenda in similar timeframes has put pressure on budgets."

"Even though grants have assisted with the latter," Ms. Biondi concludes, "the funding has been nowhere near enough to deal with all the technical, operational, systems change, management and administrative costs involved. The FOIA's real challenge is changing the mindset from one of non-disclosure to total transparency as the public monitor what civil servants, council officials and others are doing on their behalf."

A recent eGovernment survey supports Ms. Biondi's claims. This survey indicated that a third of public sector bodies believe their internal information handling systems will struggle to implement the new legislation. More alarmingly, other recent surveys reveal that just 17% of local authorities have set aside budgets to implement electronic systems that comply with the Act, highlighting the lack of preparedness. Even those organisations that have successfully developed FOIA policies and procedures may not have implemented the technology that can ensure that the requirements of the Act are met. In fact, a recent survey has revealed that local government organisations believe their current document handling systems will not be up to meeting their FOIA procedural requirements.

Records-management issues and their affect on FOIA compliance

Because many of these organisations do not yet have FOIA-compliant processes and/or technology in place, typical records management issues faced by most organisations become more pronounced. For instance, think about how some of the following, common catalysts for records-management problems - according to the research report, "The CIO's Guide to Effective Records Management," published by the Gartner group - are going to be affected now that even more attention will be focused on organisations' records-management and information-retrieval capabilities:

- *Lack of centralised document oversight* — Documents are often created in decentralised, unsupervised environments. The environments tend to be departmental or functionally focused, with little corporate-level regulation or broad attention to formal document life-cycle management.
- *Lack of standardised naming conventions* — Documents are given names that make sense to their authors and users, but not to anyone else. The lack of naming conventions, along with systematic meta-data collections or any other activity that facilitates the transition from live document to corporate record, can slow down or lessen the accuracy of data searching and retrieval.
- *Lack of logical file structures* — Document filing strategies are too often left to the whims of individual preference, with file folders and taxonomies are created idiosyncratically or on an ad hoc basis.
- *Unnecessary document duplication* — Because many important documents are not stored centrally, they may be subject to duplication, a profound indication of having no RM capability at all.

Not only do the general procedural issues listed above need to be addressed, but the actual specific activities that drive them do as well: digital archiving, automated searching and indexing, retrieval-enhancement capabilities such as hit highlighting, and so on. Proper technology tools, when implemented correctly, can help alleviate or lessen procedural records-management inadequacies.

Technology solutions for key FOIA areas

Ian Quanstrom, managing director of ZyLAB UK, a provider of document management and full-text retrieval software, has worked with many public sector organisations in the UK, including the Metropolitan Police, to develop FOIA-compliant archiving, searching and retrieving systems.

Mr. Quanstrom explains the needs of his public-sector clients: "By definition, document imaging and paper filing software used in public sector environments must be able to digitally file and manage millions of pages of paper and electronic documents while offering high-quality search and retrieval features to a large number of users in multi-locations. The preferred solution must also offer users the ability to organise and easily share all information."

As such, when organisations make the move to become FOIA compliant, they are obviously going to need a comprehensive, yet usable and easily integrateable, solution that can handle the core functionalities that support FOIA compliance. Although each organisation may have several unique attributes that require specific types of functionality, there are certain fixed high-level activities that every FOIA process must have and which must be supported by any document management solution. In other words, at minimum, any solution must enable the document retaining body to quickly and accurately perform the following activities:

- Digital filing and automated indexing capabilities, which allow for more reliable, long-term storage of volumes of information as well as better categorisation of that information ("Digital archiving and information integrity")
- Fast information searching and compilation ("Discovery")
- Comprehensive data analysis and cross referencing, to assure the most exhaustive scrutiny of information ("Disclosure")

- The ability to "black out" sensitive bits of information within the framework allowed by FOIA ("Redaction")
- Ability to easily and quickly organise and distribute requested information ("Publishing and distribution")

Digital archiving and information integrity

Open architecture — specifically, the ability of digital archiving solutions to retain an original version of a document as an XML file – means safer storage of information and better long-term document integrity.

Aside from XML's programming and structural benefits, two advantages to XML stand out for organisations operating within an FOIA-compliant framework:

- XML is a W3C standard. (W3C is the international consortium that develops recognised standards for online operational development activities.)
- XML is an enduring and vendor-independent format—as opposed to, say, PDF—which means that users will never have to buy upgrades or additional software or worry about the technology becoming obsolete.
- Content and its associated meta-data can be stored in the same file.

Furthermore, an XML repository does not require a database, thereby offering less necessity for large integrations.

Discovery

The ability to accurately and quickly discover correct bits of archived information is arguably the single most important function driving FOIA compliance. Information cannot be bundled, analysed, redacted, or distributed if users can not readily find it.

According to a recent IDC report, "Industry Developments and Models: The High Cost of Not Finding Information", the authors discuss how "inadequate access to content is a growing problem for today's enterprises." Aside from the impact of FOIA-related retrieval issues, the inaccessibility of information affects the overall productivity of the organisation. However, these two concerns are not mutually exclusive; FOIA compliance is not intended to hinder the effectiveness of an organisation's overall operations. As the IDC report notes, "Not only is an organisation's ability to be compliant strained with inadequate search capabilities, but the overall productivity of the company is compromised." In fact, IDC estimates that:

- Knowledge workers spend 15% to 30% of their work time looking for information.
- At least 50% of online searches are not successful.
- The cost to the enterprise in lost effort, time spent recreating information that already exists, and decisions based on faulty or incomplete information is significant.

The IDC report further states that, to help alleviate such issues, "Next-generation search engines and other information finding tools have now demonstrated that they can generate significant benefits. Advanced search technologies enable users to search for and find the archived information they need with any number of techniques: Boolean, proximity, fuzzy, relevance ranking, concept search, and so on.

Disclosure

Disclosure refers to the ability to find and organise all the relevant paper-based files, notes, documents and records that are required by a requesting party. In many cases, disclosing large volumes of information can be quite time-consuming and expensive. For organisations that will engage in a high-volume of disclosure activity, they need a coordinated tool bundle, which enables them to benefit not only from advanced search techniques but also from sophisticated capabilities for quickly and accurately organising their information for easy delivery.

Redaction (de-identification)

Redaction can be a particularly tricky proposition within the practical application of FOIA in many government agencies, particularly those focused on security, intelligence, and legal activities. While the FOIA requires broad transparency and availability, that does not mean that everyone should necessarily have access to every detail of every piece of information. If one were to look at something like national security documents or high-level criminal prosecutions that rely on testimonies from protected witnesses, authorities could make a strong case for the need to redact highly sensitive information, specific dates and locations, witness names, and so on.

Certainly, any organisation must have rules and criteria in place regarding the scope, legalities and appropriateness of redaction activities. However, regardless of how the rules are implemented and carried out, some element of automatic redaction will be built in to many organisation's document and records management processes, and, given that, these organisations need as accurate and usable redaction tool as possible.

In fact, next to accurate document retrieval, redaction may very well be the biggest concern for many organisations, especially those in law enforcement, national security, or intelligence. For these types of organisations, manual redaction can account for up to a quarter of their disclosure costs.

Publishing and distribution

When the 'right to know' provisions of the Act comes into force, all public bodies, including government departments, councils, police, health and prison services, are legally bound to disclose information within 20 working days, providing there is no specific exemption preventing disclosure. On the surface, delivery of requested materials may not seem a problem: someone just compiles the information into a file, and either prints it on paper, burns it onto a CD, or distributes it through the appropriate online channel.

When one takes into consideration the points presented in the Discovery and Disclosure sections above, it becomes obvious that without the right search and retrieval tools - as well as the appropriate FOIA-compliant procedures to support them - a couple of significant distribution issues can arise:

- Quickly compiling information into a logical and organised fashion is not always easy.
- Aside from the ability to find requested information, additional components such as indexes, attachments from emails, tracking data, or so on may need to be found and made available. In addition, the final product has to be organised, readable, and, in the case of a CD, compatible with a variety of systems.

Looking at all the factors discussed in this section, one can conclude that it doesn't matter how efficient or sophisticated an organisation's publishing and distribution capabilities are if no technical capabilities are in place to quickly and accurately find, retrieve, and organise requested information, redact or otherwise control the flow of information, and safely store a wide

range of media types in a stable and open-source archival structure.

Modular solutions to FOIA compliance – a pragmatic approach

Given the common records-management problems facing many organisations (as profiled in the "Impact of FOIA on organisational activities" section above), it is imperative that with the added impetus of FOIA compliance, affected organisations must take an honest look at what they are up against in terms of expectations and the ability to meet them. Regardless of whether procedures and supporting technology are in place, public bodies will have to address records-management issues, and the sooner that happens the less risk these organisations will face.

Unfortunately, one of the main difficulties organisations have when selecting a records-management vendor is that they can often become paralysed by the perception that they have to figure out upfront every detail of the solution they need as well as the scope to which this solution must address departmental and organisation-wide issues. However, rather than engaging in the inactivity caused by as-of-yet unknown ramifications of FOIA non-compliance, organisations can embrace the general themes that are involved with any sort of records-management and information-transparency initiative, which will certainly be consistent with at least the general concepts of FOIA, and work to address those themes in whatever solution they choose.

This type of cautioned approach is possible if an array of appropriate technologies is available in modular units that can be configured and built according to the current budget and perceived level of need of an organisation. This modular approach means that organisations do not need to expend a large amount of money buying large, comprehensive "enterprise" solutions that may overshoot their actual needs; rather, a solution encompassing a measured mix of basic compliance-oriented technologies enables organisations to lay a foundation for an affordable FOIA solution on their own terms, and build upon it (or not) as they see fit.

References

- UK Department of Constitutional Affairs. The Freedom of Information Act 2000 [accessed October 14, 2004]. http://www.dca.gov.uk/foi/foiact2000.htm
- Jellinek, Dan, ed. 2004. eGovernment Outlook 2004-2005 Report. "Issue Five: Freedom of Information". Brighton, UK: Headstar.
- Logan, D., and M. Gilbert. March 2003. Gartner Tactical Guidelines TG-18-9764. The CIO's Guide to Effective Records Management.
- Feldman, Susan, and Chris Sherman. April 2003. IDC Report #29127. Industry Developments and Models: The High Cost of Not Finding Information.

Jack Vivrett is Communication Manager of ZyLAB Distribution B.V.,Amsterdam, The Netherlands

HUMOUR HALF PAGE!

On a sunny afternoon three accountants are standing near a tall pole and wondering about the height of the pole. The first accountant, an FCA says, I do not think there is any authoritative guidance on how to measure the height of a pole, that is not the job of accountants. The second accountant, a professor at a red-brick university says, well, if we take a survey of similar locations and asked people about the height of poles, then we may be able to deduce the height of this pole, it will be a good enough estimate. The third accountant is a professor at an Ivy league university. He confidently claims, if we measure the shadow of the pole under different conditions, then I can run a multivariate regression model and can give a very good estimate of the height. As this conservation is going on a computer auditor is passing by, he stops and asks about their discussion. The accountants tell him, you probably can not understand this complex problem. The computer auditor persists and hears about the problem. He smiles, lifts the pole from the base, lays it on the ground and measures it, and says, "twelve feet and three inches," and walks off. The accountants look at him, laugh contemptuously and say in unison – "we wanted to know the height of the pole and he tells us the length."

The auditors have taken an inventory of thermometers held in a warehouse, in the summer. The thermometers will be exported out of the country in January, and are kept under lock and key. In December, the auditors ask management to redo the inventory count. Management is surprised "Why? Nothing has changed." The auditors tell them "The inventory is now overstated, in summer there is more mercury in the thermometers."

IRMA

INFORMATION RISK MANAGEMENT & AUDIT

◆ A SPECIALIST GROUP OF THE BCS ◆

IRMA PRESENTATION

16:00 for 16:30 on 17 MAY 2005

at BCS, 5 Southampton Street, WC2

COMPUTER AUDIT BASICS 3 – COMPUTER AIDED AUDIT TECHNIQUES (CAATS)

The next event in our Computer Audit Basics series looks at the use of Computer Aided Audit Techniques (CAATS), and how these can be used to enhance and improve the audit work we do as well as reducing the amount of time needed to carry out audit testing.

The speaker for the evening will be Paul Fantham of Auditware Systems Ltd. Paul will explain the different types of CAATS available and the benefits of using them, and will demonstrate some of the tools available such as IDEA, IDEA Server, Unix Security Auditor, XDrill and Wizrule.

The Computer Audit Basics 3 session will be useful for anyone who would like to learn more about CAATS or improve the way they carry out audits by using the automation that modern tools can provide. It should be especially worthwhile for anyone studying for BCS, IIA or ISACA qualifications or wishing to earn CPE hours. This session qualifies for one CPE hour and evidence of attendance can be provided on request.

The session will be proceeded by the IRMA AGM, which will begin a few minutes before the main event, which starts at 16:30.

To round off the evening, Alex Brewer and Ross Palmer, a duo of IRMA Committee Members, will provide some musical entertainment to go with the evening buffet, performing under the sobriquet ("*Irmacology*"). Their performance will be in the cause of sponsoring *Comic Relief*, the BBC charity that supports African and UK causes, and while neither of them have a clue at this stage what they will be doing (or even if they will both have their guitars in tune!), it should be fun – or at least laughable. More details in due course, so keep your eyes on the IRMA website.

BCS MATTERS!

Colin Thompson
BCS Deputy Chief Executive

Growing the membership

Readers may recall that back in May we launched a new BCS membership structure and a campaign aimed at attracting 10,000 new members to the Society by the end of April 2005. That was no mean target, given that the normal annual intake of new members at that time was in the order of 750. The good news is that we are well ahead of target. By the end of December we had recruited a total of 9345 new members, including 5502 new professional members and the overall membership stood at 44134 compared with 36828 at the beginning of May.

Professionalism in IT

IT skills are one of the essential elements of IT professionalism and SFIA (Skills for the Information Age) is now the de facto standard framework for those skills in the UK. The framework is owned by the SFIA Foundation whose members are BCS, IEE, IMIS and ESkills. As SFIAPlus, a more detailed version of the framework, it also forms the platform for the full range of BCS professional products such as *Skills Manager, Career Manager* and *Career Developer.*

But a skills framework like SFIA is only as good as its maintenance regime and SFIA is now undergoing its first major update since being taken over by the Foundation.

The update, being managed by BCS, will be based on widespread consultation during the next four months with IT practitioners, employers and training providers. This will ensure that SFIA continues to be an up to date common reference model for the identification of the skills required for the effective development and deployment of information systems.

The Foundation's website (http://sfia.textmatters.com/sfia) provides the facility for you to submit your comments on SFIA. It also contains the latest news about the project including details of regional workshops which you may wish to attend to contribute to the update.

New BCS Books

The past year has seen the launch of a number of new BCS titles including most recently

Business Process Management: A Rigorous Approach. The author, Martin Ould, goes beyond IT and workflow systems to focus on the interaction between processes, people and information.

A Guide to Global Sourcing, examines the opportunities and obstacles associated with offshore outsourcing and other global delivery models, and provides practical advice for IT professionals and senior managers on supervising projects successfully.

Project Management for IT-Related Projects – Textbook for the ISEB Foundation Certificate in IS Project Management, explains the principles of IT-related project management, including project planning, monitoring and control, change management, risk management and communication between project stakeholders.

A Managers Guide to IT Law is a practical book giving managers, without any specialist legal knowledge, an understanding of the law in relation to computers and IT. It explains, in plain English, the most relevant legal frameworks, with examples from actual case law used to illustrate the kinds of problems and disputes that most commonly arise.

BCS Who?

Not so long ago it was possible to find many IT professionals who claimed never to have heard of BCS. But a recent survey telephone survey conducted by an independent market research agency in November and December 2004 indicates that this position has changed very significantly. When asked unprompted to name any professional body that covers IT, 30 per cent mentioned the BCS. No other bodies registered a spontaneous recall of more than 2 per cent. When prompted with a list of six professional bodies and asked which they had heard of, the number of IT practitioners who either recognised or had heard of the BCS leapt to 62%. Interestingly, almost a third of respondents said that they had become aware of the BCS within the last 2 years, 18 per cent within the last year.

This increase is not wholly unexpected given the increase in BCS activity, both in terms of membership and more generally, and the improved quality of our marketing and PR support. But it is good to see it reflected in a survey of this kind.

Lifetime Email Address

BCS members now have access to a new email forwarding facility. The service is free to all BCS members and provides a personalised email address (myname@bcs.org.uk) from which mail can be forwarded to up to 3 other email accounts. This service allows members to maintain a single lifetime address that is independent of the point of access and of any changes in internet service provider. BCSNet accounts can now be managed online via a secure server and there is no limit to the frequency with which forwarding arrangements can be changed. The new service, has a number of enhancements over the old BCSNet service including the facility to use both the uk (@bcs.org.uk) and international (@bcs.org) versions of the BCS address. The service also comes complete with a free spam filtering facility.

To find out about getting a new account, go to http://www.bcs.org/BCS/MembersArea/EmailAddress/Registering.htm

And Free Legal Advice for members

The latest addition to the list of BCS member services is a free legal helpline. The new service, launched on17th January 2005, is provided by the DAS Group and offers advice from legal professionals on all personal legal matters - such as employment issues, consumer areas, family matters and property issues.

The new service is available 24 hours a day, 365 days a year by telephone, and there is also an email facility.

Further details are available from the members area of the BCS website.

Thought Leadership

Thought leadership debates are one of the most successful recent innovations for BCS. Designed to promote growth in, and awareness of, the underlying science, techniques and applications of IT these sessions provide opportunities that allow experts from research and practice to exchange views. The debates are strictly by invitation only, focusing on influential people who are relevant to the particular subject under discussion, and aiming to have a mixture of delegates from different backgrounds and organisations.

In the most recent of these lectures Fred Piper and Karen Sparck-Jones led the discussion on the subject 'Where is a precautionary approach to systems and software design commercially viable, or do we continue to live with reactionary measures to untrustworthiness for the foreseeable future'.

Previous debates over the past year have included 'Is network surveillance possible', 'Women in IT', 'Future vision', 'When brains meet technology', 'Designing IT for crime prevention, Ethical computing', 'Scale complexity and software and Trust and provenance'.

Reports of each of these debates can be found on the BCS Web site.

The BCS awards 2005

Over the past few years the BCS Awards have developed into the UK's leading event recognising excellence, professionalism and innovation in the IT industry. Last year's awards saw a 55% increase in entries over the year before - and the ceremony, at which 22 awards were distributed, was attended by a record near-800 people.

The awards are intended to mirror the constant changes in the IT industry. This year we are recognising developments in the rapidly growing mobile computing sector and we will continue last year's focus on women in IT, which remains as timely an issue as ever. Other categories for 2005 are:

Technology Awards entries are due *24 March*. This category focuses on excellence in computing within the context of business value and social benefit. This year, Technology Awards will be given in the following areas: Applications, Services, Systems and Social Contribution.

Business Achievement Awards entries are due *7 April*. Awards will be given to the best management team or organisation in the following subcategories: Public Sector/Not for Profit/Charitable Organisations; Financial & Related Services; Commercial & Industrial; and Small Organisations (up to 100 employees).

Individual Excellence Awards entries are due *24 June*. The subcategories include: Young IT Practitioner of the Year; IT Trainer of the Year; IT Consultant of the Year; IT Director of the Year (from organisations with fewer than 250 employees); IT Director of the Year (from organisations with more than 250 employees); Project Manager of the Year; Business Analyst of the Year; IT Developer of the Year (Applications); IT Developer of the Year (Infrastructure); and Marval IT Service Manager of the Year.

President's Awards entries are due *24 June*. Chosen every year by the BCS president to recognise timely areas of interest to the industry, this year David Morriss has selected Mobile Computing and Women in IT.

Flagship Awards include the BCS Achievement Award 2005, given to the most meritorious winner of the four business achievement awards, and the BCS Technology Award 2005, given to the most innovative medallist of the four technology categories.

Further information is available from the BCS Website http://www.bcs.org/Awards/Professional

And Finally .....

Back to the question of membership and the good news is that, as the BCS itself approaches its 50th birthday, the membership is getting younger. Latest figures show that the average age of new BCS members has fallen from 37 to 29 since May last year. In the same period the average age of all professional entrants has fallen from 40 to 33 and for new Fellows the fall has been from 58 to 43. Given that the average age has been rising for many years it really is very pleasing to be able to report that the average new entrant, and the average new professional entrant, is now within the age range for the Young Professionals Group!

Further information on these or any other BCS related issues may be found on the BCS Web site http://www.bcs.org. Information is also available from Customer Services at The British Computer Society, 1 Sanford Street, Swindon, SN11HJ (e-mail to marketing@hq.bcs.org.uk)

HUMOUR PAGE

TASK :- To Shoot Yourself In The Foot

C

You shoot yourself in the foot.

C++ You accidentally create a dozen instances of yourself and shoot them all in the foot. Providing emergency medical care is impossible since you can't tell which are bitwise copies and which are just pointing at others and saying, "That's me over there."

FORTRAN You shoot yourself in each toe, iteratively, until you run out of toes, then you read in the next foot and repeat. If you run out of bullets, you continue anyway because you have no exception handling ability.

Cobol `USE HANDGUN.COLT(45), AIM AT LEG.FOOT, THEN WITH ARM.HAND.FINGER ON HANDGUN.COLT(TRIGGER) PERFORM.SQUEEZE RETURN HANDGUN.COLT(45) TO HIP.HOLSTER.`

LISP You shoot yourself in the appendage which holds the gun with
which you shoot yourself in the appendage which holds the gun with
which you shoot yourself in the appendage which holds the gun with
which you shoot yourself in the appendage which holds the gun with
which you shoot yourself in the appendage which holds the gun with
which you shoot yourself in the appendage which holds...

Basic (interpreted) You shoot yourself in the foot with a water pistol until your foot is waterlogged and rots off.

Basic (compiled) You shoot yourself in the foot with a BB using a SCUD missile launcher.

FORTH Foot in yourself shoot.

APL You shoot yourself in the foot, then spend all day figuring out how to do it in fewer characters.

Pascal The compiler won't let you shoot yourself in the foot.

SNOBOL If you succeed, shoot yourself in the left foot. If you fail, shoot yourself in the right foot.

Concurrent Euclid You shoot yourself in somebody else's foot.

HyperTalk Put the first bullet of the gun into the foot left of leg of you. Answer the result.

Motif You spend days writing a UIL description of your foot, the trajectory, the bullet, and the intricate scrollwork on the ivory handles of the gun. When you finally get around to pulling the trigger, the gun jams.

Unix % ls
foot.c foot.h foot.o toe.c toe.o
% rm * .o
rm: .o: No such file or directory
% ls
%

XBase Shooting yourself is no problem. If you want to shoot yourself in the foot, you'll have to use Clipper.

Paradox Not only can you shoot yourself in the foot, your users can, too.

Revelation You'll be able to shoot yourself in the foot just as soon as you figure out what all these bullets are for.

Visual Basic You'll really only appear to have shot yourself in the foot, but you'll have had so much fun doing it that you won't care.

Prolog You tell your program that you want to be shot in the foot. The program figures out how to do it, but the syntax doesn't permit it to explain it to you.

370 JCL You send your foot down to MIS and include a 400-page document explaining exactly how you want it to be shot. Three years later, your foot comes back deep-fried.

Apple We'll let you shoot yourself, but it'll cost you a bundle.

IBM You insert a clip into the gun, wait half an hour, and it goes off in random directions. If a bullet hits your foot, you're lucky.

Microsoft Object "Foot" will be included in the next release. You can upgrade for $500.

Cray I knew you were going to shoot yourself in the foot.

Hewlett-Packard You can use this machine-gun to shoot yourself in the foot, but the firing pin is broken.

NeXT We don't sell guns anymore, just ammunition.

Sun Just as soon as Solaris gets here, you can shoot yourself anywhere you want.

Ada After correctly packing your foot, you attempt to concurrently load the gun, pull the trigger, scream, and shoot yourself in the foot. When you try, however, you discover you can't because your foot is of the wrong type.

Access You try to point the gun at your foot, but it shoots holes in all your Borland distribution diskettes instead.

Assembler You try to shoot yourself in the foot, only to discover you must first invent the gun, the bullet, the trigger, and your foot.

Modula2 After realizing that you can't actually accomplish anything in this language, you shoot yourself in the head.

csh After searching the manual until your foot falls asleep, you shoot the computer and switch to C.

dBase You buy a gun. Bullets are only available from another company and are promised to work so you buy them. Then you find out that the next version of the gun is the one that is scheduled to actually shoot bullets.

PL/1 After consuming all system resources including bullets, the data processing department doubles its size, acquires 2 new mainframes and drops the original on your foot.

HTML Shoot here

Java The gun fires just fine, but your foot can't figure out what the bullets are and ignores them.

MOO You ask a wizard for a pair of hands. After lovingly handcrafting the gun and each bullet, you tell everyone that you've shot yourself in the foot.

Smalltalk You daydream repeatedly about shooting yourself in the foot.

FTP ftp lower-body.me.org
ftp> cd /foot
ftp> put bullets

DCL You manage to shoot yourself in the foot, but while doing so you also shoot yourself in the arm, stomach, and leg, plus you shoot your best friend in the chest, the neighbour's dog and your car. A month later you're not able to understand your program anymore when you read the source.

Windows95
d:\setup

(Therefore proving that COBOL is still the most elegant, sensible and understandable of all the languages – Ed)

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

Member Benefits Discounts

Mark Smith

This quarter's discounts include a Unicom event that may be of interest: "Sarbanes-Oxley for IT Auditors and Management" on 7th and 8th April. The usual cost of attendance is £595+VAT per day, but IRMA Members can claim a discounted rate of £275+VAT a day! See www.unicom.co.uk for more details.

Another new offer is a 15% discount off MIS Training's "Audit & Control of Information Technology & Systems" event on 17th-18th May. The IRMA Chairman, Alex Brewer, will be one of the speakers. See www.mistieurope.com for further information.

Other discounts we have negotiated are listed below:

Software

Product	*Discount Negotiated*	*Supplier*
Caseware Examiner for IDEA (mines security log files for Windows 2000, NT, XP)	15%	Auditware Systems (www.auditware.co.uk)
IDEA (Interactive Data Extraction and Analysis)	15%	Auditware Systems (www.auditware.co.uk)
Wizrule (data auditing and cleansing application)	20%	Wizsoft (www.wizsoft.com)
Wizwhy (data mining tool)	20%	Wizsoft (www.wizsoft.com)

Events

Event	*Discount Negotiated*	*Contact*
Audit & Control of Information Technology & Systems (www.mistieurope.com)	15%	Lisa Davies LDavies@mistiemea.com
Computer and Internet Crime 2005 (www.cic-exhibition.com)	15%	Paul Webster paul@panpres.co.uk
IACON 2005 (17th & 17th March)	20%	Jonathan Harvey jharvey@iirltd.co.uk
All Unicom events (www.unicom.co.uk)	20%	Julie Valentine julie@unicom.co.uk

We are looking to extend this range of discounts to include additional events, training courses, computer software or other products that our members may find beneficial. If you have any suggestions for products we could add to the list, please contact Mark Smith (mark.smith@lhp.nhs.uk), our Members' Benefits Officer, and he will be happy to approach suppliers.

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 — 4 = Academic 2 = External Audit — 5 = Full-Time Student 3 = Data Processor — 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	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

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

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

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	Alex Brewer	alex.brewer@morganstanley.com
SECRETARY	Siobhan Tracey	siobhan.tracey@booker.co.uk
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Celeste Rush	rushlse97@aol.com
JOURNAL EDITOR & SECURITY PANEL LIAISON	John Mitchell	john@lhscontrol.com
WEBMASTER	Allan Boardman	allan@internetworking4u.co.uk
EVENTS PROGRAMME CONSULTANT	Raghu Iyer	raguriyer@aol.com
LIAISON - IIA & NHS	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON - LOCAL AUTHORITY	Peter Murray	cass@peterm.demon.co.uk
LIAISON - ISACA	Ross Palmer	ross.palmer@hrplc.co.uk
MARKETING	Wal Robertson	williamr@bdq.com
ACADEMIC RELATIONS	David Chadwick	d.r.chadwick@greenwich.ac.uk
	David Lilburn Watson	dlwatson@bcrm.co.uk

SUPPORT SERVICES

ADMINISTRATION	Janet Cardell-Williams t: 01707 852384 f: 01707 646275	admin@bcs-irma.org
OR VISIT OUR WEBSITE AT	**www.bcs-irma.org**	Members' area Userid = irmamembers Password = irma2004

BCS IRMA SPECIALIST GROUP ADVERTISING RATES

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: admin@bcs-irma.org
Website : www.bcs-irma.org

BCS IRMA Specialist Group Advertising Manager

Eva Nash Tel: 01707 852384
Email: admin@bcs-irma.org

Venue for Full Day Briefings

BCS, The Davidson Building,
5 Southampton Street,
London WC2 7HA