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

JOURNAL
VOLUME 17 NUMBER 3 AUTUMN 2007 ISSN 1741-4229

BCS
THE BRITISH COMPUTER SOCIETY

Programme of Briefings & Meetings 2007-8

Date	*Subject*	*Speaker*	*Time*	*Location*
2007				
9 Oct	Computer Crime Update	Peter Wood, Daniel Cuthbert Sarb Sembhi, John Mitchell	Full Day	BCS London Office
6 Nov	Electronic Autopsy (digital forensics)	Ian Kennedy	17:30	BCS London Office
11 Dec	Inside the Mind of Convicted Fraudsters	Sean Holohan	17:30	BCS London Office
2008				
8 Jan	Data Quality (joint meeting with the Data Management SG)	Keith Gordon	17.30	BCS London Office
5 Feb	Handling computer-related incidents in the workplace	Jan Collie	17.30	BCS London Office
14 Feb	Software auditing (joint meeting with the Advanced Programming SG)	John Mitchell	17.30	BCS London Office
4 Mar	Critical National Infrastructure	TBA	17.30	BCS London Office
1 Apr	RFID	Ken Munro	17.30	BCS London Office
27 May	AGM + TBA	TBA	17.00	BCS London Office
10 June	TBA	TBA	17:30	BCS London Office
1 July	TBA	TBA	17:30	BCS London Office

Apart from some joint meetings with other organizations all meetings will be held at BCS, 5 Southampton Street, London WC2 7HA
This is a draft programme only and is subject to change. For confirmation of dates and further information,
watch the **Journal**, email **admin@bcs-irma.org** or visit our website at **www.bcs-irma.org**

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 delegate's pack.
For venue map see back cover.

Email distribution is here . . .

IRMA has moved from paper to electronic distribution of the Journal, so we need your email address! If you have not already supplied it, please can you send your email address to our admin office at admin@bcs-irma.org – Many thanks.

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

PLEASE NOTE THE EMAIL ADDRESS FOR

IRMA ADMIN IS:

admin@bcs-irma.org

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

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
john@lhscontrol.com

Produced by Carliam Artwork,
Potters Bar, Herts

Editorial

John Mitchell

John Ivinson who was involved with the early days of IRMA, then the Auditing By Computer SG, died a few months ago. John eventually became BCS President and was also the founding President of ISACA London Chapter. You can read an obituary elsewhere in this edition. It's been one of those quarters when things keep going wrong: Tax self assessment, VAT refunds, broadband speeds that aren't, poor configuration management killing people and the Electoral Commission stating that the Government should forget about electronic voting. Finally, there was an interesting comparison between the US and the UK on hospital waiting times. Strangely enough, I have been involved with all of these incidents. Perhaps it's my profession which makes me note control issues in much the same way as train spotters collect engine numbers.

First, a word of warning about the Revenue & Customs self assessment tax scheme. It cannot calculate twenty percent of an odd number for gains on UK life policies. When I confirmed this with their support desk they agreed there was a problem. That was two months ago as I write this and the problem remains. Moral of the story: always check the derived data from a calculation. Then I received a welcome, but unexpected cheque from the VAT side of the organisation. Straight into the bank while I investigated. I pay my VAT by direct debit so I assumed that I had been debited twice and the cheque was the refund. Not so. Another call extracted an apology. They had processed a batch of VAT returns twice and therefore must have debited me twice, hence the refund with apologies. Not so stated I and they eventually called back to agree. Could I now pay them some money please as they had only taken it once and the refund cancelled it out? Moral of the story: always check your correction controls just in case they don't.

For some time I have been using BT's up to 8 megabyte broadband. I have never, ever, achieved anything better than 1.5 megabyte which BT say is okay because they advertise "up to 8 megabyte". As far as my limited research has shown this can only be achieved if you are located right next door to an exchange and have a direct fibre link. At last Ofcom and the Advertising Standards people are beginning to take note after a damning report from the consumer group Which? Moral of the story: "up to" really equates to "up yours". Then the Electoral Commission published their report on the recent electronic voting pilots. Pretty damming all round and with a recommendation that the Government should sort out some fundamental issues before trying again. Regular readers of this column will be aware of my views on the subject and I have written to the Commission several times on the subjects of confidentiality, integrity and availability. Interestingly, it is not on these issues that the Government is likely to act, but the cost. At £800 per participating voter, it's hardly cost effective either. Moral of the story: simply getting people to vote is no good if you can't rely on the result.

The sad news that two patients had died as a result of a radiation overdose whilst undergoing cancer treatment reminded me that I had raised this as a potential issue in a recent lecture on data management. These devices are computer controlled and parameter driven. Moral of the story: get the parameter data wrong and people die. Finally, having spent numerous hours in various NHS queues I was interested to read that, in the US, after a hospital promised to see emergency patients within fifteen minutes of arrival, a competing hospital rolled out a programme promising two cinema passes if you are not attended to within thirty minutes. "Over the next five years you'll see this pretty much everywhere except in the smallest hospitals," said Rick Wade, spokesman for the American Hospital Association. I wonder what your dependents will get if you die while waiting? Moral of the story: competition is usually better than state ownership in reducing waiting times.

In this issue we have an article from Glen Gray on XBRL. None the wiser of its importance, then read the article? Craig Write discusses the problems associated with document destruction and we have our regular contributions from Ross Palmer our Chairman, Bob Ashton our Oceana correspondent and Andrea Simmons updating us on the Security Strategic Forum.

OBITUARY

John Ivinson, former BCS President 2002-3 and an early member of IRMA when it was the Auditing By Computer specialist group, passed away on 11 July 2007 at the age of 63.

According to BCS chief executive, David Clarke, 'John was an exuberant and colourful figure within BCS circles. He loyally served the BCS during his presidential term and because of his long term commitment to the Society and its various activities, he commanded a great deal of respect across a broad sector of our membership. He was very knowledgeable about the BCS and was a particularly valuable source of information on the history of British computing.'

Professor Nigel Shadbolt, current BCS President added, 'John regularly attended most major BCS events; he gave huge amounts of his time and energy to the BCS. He was a very popular character amongst his wide circle of friends and acquaintances and he will be greatly missed. Our sympathies are extended to his partner Janet with whom he shared his life; also to his son Robert.'

John Ivinson had worked in IT since 1967 - after graduating in geography and American studies. He was a consultant since 1972, working for a wide variety of organisations nationally and internationally, especially in system development, computer audit and project management.

He was a technical consultant to the UK government's Action 2000 body for the year 2000 systems issue, and joint director of the government's year 2000 Bug Busters Scheme. He joined the BCS in 1967 and held many posts, including chairman of the Technical Board, the Royal Charter Committee, the International Policy Committee and the Professional and Public Affairs Board.

John sat on the DTI working party for the creation of an accredited certification scheme for BS7799 (Information Security Management) and on the BSI Committee for the Standard. He also wrote a report commissioned by the DTI on the IT-skills shortage problem, a perennial problem for the IT Profession, and acted as a one time Specialist Adviser to the House of Commons Select Committee on Science and Technology.

Not surprisingly, IT was not the only area where John Ivinson was active: he was formerly Honorary International Treasurer of the International Food & Wine Society and remained an active member until his death. His interests outside food and wine included listening to jazz, reading detective novels and skiing.

Letter to the Editor

Dear Editor,

In response to your continued requests for volunteers, I am in the process of changing jobs so I wouldn't want to commit to arranging events in the North at the moment – but I might be able to assist in the future.

I'm well aware of the difficulty of getting volunteers for anything, but being someone who often does volunteer, I also know I'm probably overstretched right now.

Of course the BCS does have a local branch, but their events are generally not IRMA related; and as far as I can tell the north branch of the ISACA (of which I am also a member) is also virtually dormant, but both may offer a pool of attendees.

Leeds is of course the largest Financial Services centre in the country outside London so if events were run in the north, with the number of IT Auditors in FS, there must be a market here.

I will get involved in the London activities if I can, but I probably spend 10 days a year in London and if it doesn't overlap with another reason to go, it's very hard to justify the time.

Regards,
Matt Palmer

Chairman's Corner

Ross Palmer

Matters of Identity

Michael Parkinson once asked Morecambe and Wise what they would have been were they not comedians.

"Mike and Bernie Winters!" was Eric's quick-witted reply (which will probably only mean something to those who, like me, were born too early to enjoy "Grange Hill" while still being at school).

That was a very funny gag, but the ability to align with the personal characteristics of another (outside of the acting profession) is a dubious skill and history is littered with attempts to distance oneself from one's own identity or to associate with somebody else's, for whatever reason:

- (Greed) The "Advance Fee Fraud", aka the "Nigerian scam", where a con artist claims to be a Nigerian nobleman with millions of dollars locked up in a bank account or inheritance fund which he cannot touch without your help and "minor" investment for release fees, and for which you will be amply rewarded …
- (Principle) The Cambridge Five spy ring – Philby, MacLean, Burgess, etc. - who felt the need to betray their own country to a Communist regime;
- (Hunger) The wolf that tried to pass itself off as Red Riding Hood's granny, (although I'm now coming to understand that this story may be apocryphal).

Identity theft has become a significant scourge of our society in recent years. Why, 25 years ago, we would not have thought twice about casually disposing of bank statements, utility bills, old cheque stubs, etc. after just tearing them in half.

Even today, we issue cheques to people we don't know (I suppose thinking that any risk lies with the recipient). But cheques provide a host of one's bank details:

- bank account name and number;
- branch name, address and sort code;
- account holder's signature.

This is arguably compounded by the "horrifying" number of companies, government departments and other public bodies that have breached data protection rules in the past year, according to a report by the UK's Information Commissioner, Richard Thomas, which found:

- a total of 12 high street banks guilty of discarding customers' personal details (including bank statements, cut up credit cards and loan applications) in unsecured bins outside their premises;
- problems with shared logins at a prominent call centre and with temporary passwords at a Government agency.

On the face of it, respect for customer privacy appears not always to be at the desired level and members of the public need to be fully aware of this and take positive steps to preserve their own identities.

However, ID theft has now taken on a far more sinister turn than mere greed or principle and it is endangering our younger generation who are unwittingly complicit, particularly through self-publicising websites such as MySpace and YouTube.

Since teenagers were "invented" in the 1950s they (we) have naturally wanted to be highly thought of and "respected" amongst our peers… and who wouldn't? In many innocent ways we try to attract attention. We all like to be liked, innit?

Unfortunately, the psychological filter for excluding, or at least identifying, the undesirables (like the wolf, above) is seldom uppermost in the mind of a young, free spirit and this gap in the audience profile too often becomes filled by that 21st century blight – the "stalker" and his/her "grooming" techniques.

The lack of correlation between technology-savvy youth and an adequate degree of caution is the subject of an excellent, but disturbing, research paper written by Andy Phippen and Steven Furnell, entitled "Raising a Generation at Risk?", which is published on the BCS Security portal.

"School's out for Summer…"

… and so is IRMA, with no more seminars until October 9th, when an all-day joint event will be held with ISACA (London Chapter) on the subject of "Computer Crime Update" – check out the detail on the www.bcs-irma.org website.

Regretfully, for personal reasons, I shall be unable to attend, but it looks to be a good day with high-profile speakers on phishing, hacking, RIPA and computer forensics … all the "nasties", if you like.

I have also been told that, when booking, my normal response of "large portions please" is not a valid answer to the special dietary requirements question.

Finally – My Frozen MP3

For no apparent reason, my MP3 player, upon which I rely for motivation as I walk to work, "froze" for no reason recently. I had to look on the web for the solution, which involved shoving the end of a paper clip in the reset/reboot hole (all the time hoping "reset" did not mean "total delete").

So, now I need to keep a paper clip about my person at all times – but where to keep it, I thought?

The answer came flooding back from a concept from my childhood – the proverbial clip round the ear!

Have a great remainder of summer and let's hope the record-setting floods that caused so many problems in July were a one-off.

IRMA MEMBERS' BENEFITS DISCOUNTS

We have negotiated a range of discounts for IRMA members, see 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
E-Tec courses (www.e-tecsecurity.com)	10%	Margaret Mason (info@e-tecsecurity.com)
IACON (www.iir-iacon.com)	20%	Jonathan Harvey (jharvey@iirltd.co.uk)
All Unicom events (www.unicom.co.uk)	20%	Julie Valentine (julie@unicom.co.uk)

We are constantly 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@smhp.nhs.uk), our Members' Benefits Officer, and he will be happy to approach suppliers.

The Down Under Column

Bob Ashton – IRMA Oceania Correspondent

New Zealand Banking

The New Zealand Bankers Association has recently re-issued its Code of Banking Practice, which is now in force. Rules relating to Internet banking have been tightened considerably, the root intention of which appears to be a desire on the part of the banks to shift the liability for losses resulting from internet banking fraud from themselves to their customers. The Code states that customers will be liable for losses if they have: "*failed to take reasonable steps to ensure that the protective systems such as:*

- *virus scanning*
- *firewall*
- *anti-spyware*
- *operating system and*
- *anti-spam software on your computer are up to date.*"

It goes on to back this up by stating: "*We reserve the right to request access to your computer or device in order to verify that you have taken all reasonable steps to protect your computer or device and safeguard your secure information in accordance with this Code. If you refuse our request for access then we may refuse your claim.*"

As all banks in New Zealand are members of the Association and subscribe to the Code, then the only option for a customer who did not agree with these new impositions would be to stop using Internet banking.

Up until the present, banks have reaped great benefits resulting from the reduced costs of conducting transactions through Internet banking because of staff reductions and branch closures. Indeed the customers have disproportionately born the costs in terms of both hardware and software. For their part the banks have largely accepted the losses suffered by consumers resulting from internet banking frauds as a cost of doing business through this channel, and have guaranteed that they would make up for any losses caused by the compromising of user accounts.

In recent years internet banking fraud losses have increased dramatically. The banks may therefore feel justified in placing a greater responsibility on their customers to take reasonable precautions than has previously been the case. The transfer of liability from the banks to the customer is a harsher way of describing this.

The "*up to date requirement*" requirement is on examination both vague and onerous. Any computer running a non current operating system such as a home computer running Windows 2000 would fail this test, as would one running a current release of software that had not had all the latest patches applied. It is unlikely that naïve home users would be able to fulfil these requirements. Indeed, well run businesses would not either, as it is wise to properly test vendor supplied patches and upgrades before they are placed in the production environment, and this process takes time. Also, businesses typically run legacy software which they know to be stable. Indeed, this is the practice of many banks.

The other major objection to this regime is the ability to invade the privacy of their customers which the New Zealand banks have appropriated to themselves. It is unlikely that home users or businesses would welcome the prospect of bank officials trawling through the confidential information held on their hard drives in the hope of catching them out on some piece of software which was not in the bank's opinion fully up to date.

The great majority of banks in New Zealand are wholly owned subsidiaries of Australian banks, so Australian customers should not be surprised to subject to similar impositions in the not too distant future, although the Banks have indignantly denied that this is their intention. No doubt banks in other countries will be closely monitoring these developments.

For further information: www.nzba.org.nz

Security Forum Strategic Panel Update

Andrea Simmons

Identify Yourself

Since I last had the opportunity to communicate with you, there have been many events and meetings to attend and many opportunities to contribute to consultations etc, the main driving force behind which appears to have been either related to Resilience (the sexier term for Business Continuity methinks?) or Identity Management. Sufficient is the level of interest in the latter that I thought I would bring the following to your attention in the hopes of not duplicating communication you may have already received but to be able to channel and co-ordinate a robust BCS response.

The EURIM Personal Identity Group hosted a workshop on 20th July with the Head of Standards for the Identity and Passport Service. As referenced in their July newsletter, "The aim is to establish an independent Identity management standards group. The focus will be on how to promote shared understanding of identity assurance requirements, to help maximise interoperability between systems, maintain integrity of identity data, improve efficiency and foster trust". A tall order! It continues "The standards adopted will need to be fit for purpose and adapted to business risk. The governance of the overall Identity management Strategy Group is expected to involve senior officials from across government, chaired by a permanent secretary (or equivalent) and to have links to the appropriate standards groups." Naturally, the BCS wish to be heavily embedded in this process.

Therefore, please do get in touch if you would like any more background information and if you would like to be represented on each or any working group, as identified below:

1) technical standards
2) data standards
3) process standards
4) mapping (scope and objectives) – seeking to achieve a repository of relevant standards, building on what already exists, before the end of 2007.
5) information assurance standards.

BCS Security Forum are naturally keen to be actively involved in these activities, particularly the mapping exercise so that we can identify what exists already rather than building separate wheels. I believe this piece should feed into the other groups identified. I know that you are all learned colleagues and will be able to furnish me with information relating to standards already in existence around identity management and assurance – all offers of suggestion gratefully received. e: andrea.simmons@bcs.org

The International Association of Privacy Professionals (IAPP) recently ran a "tell us in 100 words or less" competition to come up with the best description of what a Privacy Professional is – and the result was the following:

> **A Privacy Pro Is. . .**
> "a leader who understands the technical, legal and operational aspects of gathering, handling and securing personal data, and who can establish and maintain a comprehensive strategic vision for handling all personal data of employees, customers and suppliers of an organization in a manner that is legal, secure and ethical, from the point of acquisition through the point of disposition, thereby gaining public trust in the organization's role as custodian of such data."

Is this beyond the wit of a security professional or do you believe that it is intrinsic to our intentions? Again, answers on a postcard!

If you don't already subscribe to Bruce Schneier's Counterpane newsletter, available monthly, I can highly recommend it as a good resume of articles and activity of interest in the security space, internationally, during the preceding month. www.counterpane.com His last newsletter equally had a privacy flavour to it and the following struck a chord:

> We need to build systems with privacy-enhancing technologies that limit data collection wherever possible. History will record what we, here in the early decades of the information age, did to foster freedom, liberty and democracy. Did we build information technologies that protected people's freedoms even during times when society tried to subvert them? Or did we build technologies that could easily be modified to watch and control? It's bad civic hygiene to build an infrastructure that can be used to facilitate a police state.
>
> *Bruce Schneier, July 2007*

Other news

The BCS Security Forum is continuing to forge stronger working relationships with groups like EURIM, Intellect and the Cyber Security KTN (now funded by DBERR, formerly DTI). The latter have recently been involved in the development of a work package that will sponsor a £10m, 3 year research and development programme into how to balance the potentially intrusive nature of identity services and network security with users' expectations of privacy and consent. So if you are working for a company that has developed appropriate PET's (Privacy Enhancing Technologies) again, do get in touch. The KTN are keen to identify opportunities for seed funding etc.

In terms of joined up working, the Ethics, Health and Security Forums are joining forces for an event on 2nd October 2007 at BCS Southampton Street, focusing on data privacy with the three strands represented by the three forums covered by way of content and speakers. Make a note in your diary and watch out for more bulletins regarding this. It is hoped that we will all be able to do more of this kind of joint working across the various forums representing specialists groups and otherwise, in order to provide a more holistic approach to servicing the charter requirements of the BCS, addressing contentious issues of the day in a manner that encompasses all, wherever possible, rather than perpetuating a silo'd mentality.

And of course, the week after on 9th October is the IRMA **Computer Crime Update**, joint event with ISACA, which goes to prove this "joint working" is really bearing fruit.

Finally, if you have a news item that you would like to bring to the attention of the membership, again please do get in touch as the various communication mechanisms are always keen for content. And there will be the opportunity to contribute to a Security Forum podcast in the future too – either visually (i.e. in front of camera) or aurally (by way of an audio recording at a time and place to suit you). Happy to hear from you on any related matters.

Sir Robert Peel's Nine Points of Policing

When Sir Robert Peel created the world's first regular police force he wrote down the underlying principles of policing. I believe that these principles are still relevant today to everyone involved in crime prevention and detection. Ed.

☛ The basic mission for which the police exist is to prevent crime and disorder.

☛ The ability of the police to perform their duties is dependent upon public approval of police actions.

☛ Police must secure the willing co-operation of the public in voluntary observance of the law to be able to secure and maintain the respect of the public.

☛ The degree of co-operation of the public that can be secured diminishes proportionately to the necessity of the use of physical force.

☛ Police seek and preserve public favour not by catering to public opinion but by constantly demonstrating absolute impartial service to the law.

☛ Police use physical force to the extent necessary to secure observance of the law or to restore order only when the exercise of persuasion, advice and warning is found to be insufficient.

☛ Police, at all times, should maintain a relationship with the public that gives reality to the historic tradition that the police are the public and the public are the police; the police being only members of the public who are paid to give full-time attention to duties which are incumbent on every citizen in the interests of community welfare and existence.

☛ Police should always direct their action strictly towards their functions and never appear to usurp the powers of the judiciary.

☛ The test of police efficiency is the absence of crime and disorder, not the visible evidence of police action in dealing with it.

THE BRITISH COMPUTER SOCIETY
Budget totals 2007/08

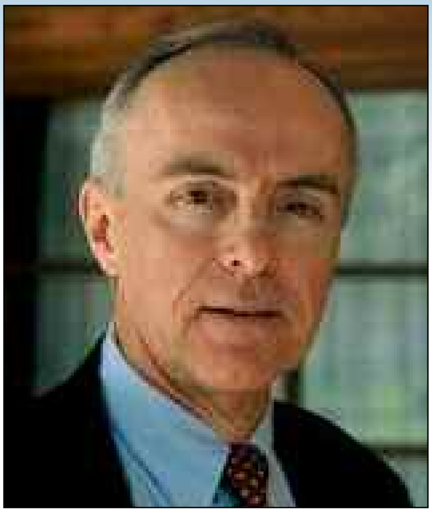
Cost Centre Budget Comparison	IRMA	Income	£2,795
As of July 31, 2007		Expenditure	£4,165

Account	*Description*	*Period Actual*	*Period Budget*	*Variance*	*%*	*YTD Actual*	*YTD Budget*	*Variance*	*%*
Income									
1708	Events Registration Fees		20.00	(20.00)	(100.00%)		40.00	(40.00)	(100.00%)
1903	Membership Subscriptions (SGs)					25.00		25.00	
Total Income			**20.00**	**(20.00)**	**(100.00%)**	**25.00**	**40.00**	**(15.00)**	**(37.50%)**
Expenditure									
3010	Travel/Subsistence (Other)	50.00	50.00	100.00%					
4000	Stationery	332.32	400.00	67.68	16.92%	332.32	400.00	67.68	16.92%
4130	Speakers expenses	20.00		(20.00)		20.00	200.00	180.00	90.00%
4150	Catering	93.36	125.00	31.64	25.31%	338.35	375.00	36.65	9.77%
4210	Seminars & Conferences					74.77		(74.77)	
4980	Administrative Services (SGs)					56.08	600.00	543.92	90.65%
Total Expenditure		**445.68**	**525.00**	**79.32**	**15.11%**	**821.52**	**1,625.00**	**803.48**	**49.44%**
Overhead Allocation (Charge)									
	Total Overhead Allocation (Charge)								
Overhead Allocation (Credit)									
	Total Overhead Allocation (Credit)								
Grand Total		**(445.68)**	**(505.00)**	**59.32**	**11.75%**	**(796.52)**	**(1,585.00)**	**788.48**	**49.75%**

Using XBRL — Audit and Control Implications

Extensible business reporting language, commonly known as XBRL, standardizes the way organizations collect, prepare, and share business information. However, organizations and internal auditors need to become acquainted with the different control issues that might impact XBRL use and its effectiveness.

GLEN GRAY, PH.D., CPA
Accounting and Information Systems Department,
California State University at Northridge



According to Charles Hoffman, the founding father of XBRL and the director of industry solutions and financial reporting for UBmatrix, the benefits of XBRL extend beyond the creation of end reports and touch all aspects of the information supply chain. XBRL standardizes data formats through the use of agreed-upon tags (a type of metadata involving the association of descriptors with objects), simplifying the way data is imported, converted, and presented in business and financial reports. "Using XBRL streamlines the work for internal auditors and enables organizations to reduce reporting errors and risks," explains Hoffman.

"XBRL is an application of extensible markup language (XML) to business data that uses standardized tags to describe this information, thus making business information immediately reusable and interactive," says Mike Willis, a partner with PricewaterhouseCoopers (PwC) and the founding chairman of XBRL International, a consortium of more than 500 companies and agencies worldwide that build XBRL and promote and support its adoption. "Because XBRL is an Internet-based information standard, it enables the seamless flow of information from one organization to another, as well as the customization of data for different reporting purposes," he adds.

A Brief History of XBRL

1998 While researching XML for financial information reports, Charles Hoffman begins to develop prototypes of financial statements and auditing programs using XML. Later that year, the American Institute of Certified Public Accountants (AICPA) is made aware of the work, and its “High Tech Task Force” proposes the creation of a prototype for financial statements using XML. The project is granted financial backing by the AICPA.

1999 The prototype is completed and presented, describing XML as important for the accounting profession. AICPA requests business plan to perform research into the commercial potential of XML and names the project XFRML. The first meeting is held at AICPA in New York in October 1999.

2000 The name of the organization is officially changed to XBRL. The XBRL committee announces the presentation of the first specification for financial statements for American businesses. The membership of the committee increases significantly.

2005 The Federal Reserve Board and the Office of the Comptroller of the Currency launch an XBRL campaign involving quarterly bank statements from 8300 U.S. Banks.

2006 A white paper is released describing the FDIC project as huge success.

Because XBRL uses common templates for the analysis of business reports, many internal auditors are taking the lead in converting the outputs of dissimilar systems into XBRL documents as a way to maximize audit review efforts. However, before embarking on an XBRL initiative, auditors need to be aware of the different audit and control issues associated with its use, especially for created end reports that require internal audit assurance. Armed with this knowledge, auditors will be able to maximize XBRL use and add more value to companywide information supply chain activities.

AUDIT AND CONTROL ISSUES

Although the application of XBRL has the potential to improve data analysis, accelerate the use of continuous auditing, reduce the proliferation of spreadsheets throughout the information supply chain, and enhance two-way audit trails, internal auditors interested in the use of XBRL need to be cognizant of the different challenges associated with its use. (For more information about the internal audit benefits of XBRL, read *ITAudit's "Got XBRL?"* article, published on June 10, 2007.)

"The good news about XBRL is that it allows organizations to create, publish, and consume detailed business information through the use of clear text and standardized tags," comments Eric E. Cohen, XBRL technical leader for PwC. "The bad news is the good news — that XBRL data is easy to create, publish, and consume, thanks to the use of clear text and standardized tags." According to Cohen, this is because XBRL could be used for industrial espionage or other nefarious purposes unless appropriate security measures are implemented such as XML signatures and encryption. “Although this is a temporary challenge, it is a challenge nonetheless,” Cohen adds.

In 2002, the Canadian Institute of Chartered Accountants (CICA) published a report, *Audit & Control: Implications of XBRL* (PDF, 204 KB), that describes three kinds of risks organizations may face when using XBRL for financial reporting — risks of errors, control issues, and assurance issues. Although CICA describes these risks as part of the financial reporting process, these risks can impact other kinds of business reporting as well. Below is a description of each risk and recommendations internal auditors can provide to organizations interested in implementing XBRL.

Risks of Errors

Error risks center around the accurate mapping of business information to tags and the use of appropriate taxonomies (i.e., XBRL dictionaries that define the specific tags for individual items of data). Hence, mapping tags accurately ensures that the data retrieved is correct. Consequently, without an effective internal control structure to ensure accurate tagging, the data retrieved can represent invalid and inaccurate transactions.

The importance of accurate tagging and mapping of information is increased when data is streamed in real time and automated; the risk of error in the statement or report increases, depending on existing change management controls and the effectiveness of the controls that oversee changes in the mapping of data to tags. This also creates additional risks because the data mapped to a particular tag may change without the organization's knowledge due to a faulty control, which increases the likelihood of errors. As a result, when XBRL instance documents are generated in real time, tests of the mapping algorithms captured in the conversion software used to turn business data into tags must be comprehensive to ensure that the converted information retains its accuracy and integrity.

Control Issues

XBRL control risks pertain to the use of appropriate taxonomies, tagging of data, and the integrity of the tagged data. "Ensuring that the client has used the appropriate taxonomy in the creation of their filings or financial reports is a major audit and control issue," explains Diane Mueller, vice president of XBRL Development for JustSystems Inc. and a member at-large of the XBRL International Steering Committee. "Auditors, therefore, must be aware of the different taxonomies in existence and ensure that the appropriate one is being used." (To see the U.S. Financial Reporting Taxonomy Framework overview, click here.)

Once the appropriate taxonomy is chosen, the next area of risk is the actual tagging of data. "Taxonomies can be complex hierarchies and contain thousands of concepts," Mueller continues. "Correctly choosing what information to map to each tag can be difficult when learning how to navigate the tools and taxonomies in the tagging process." For example, organizations need to have a system in place that ensures the appropriate taxonomy was chosen when preparing a financial statement. Therefore, staff working on the business report need to be knowledgeable about the requirements of a particular report and the taxonomy used so they can pick the right taxonomy. Otherwise, the organization runs the risk that tags are implemented incorrectly, which affects the accuracy of the reported information throughout the entire information supply chain.

When reviewing the taxonomy for its appropriateness, auditors should review the details of the taxonomy to determine whether they are up-to-date with current business and reporting requirements and whether the taxonomy is applied correctly. In addition, auditors need to determine whether there are procedures in place to ensure that the tagging of data is complete and accurate. These procedures include review and approval activities by a knowledgeable person on:

- The tagging that is applied.
- The data elements to which tags are applied.
- The consistency of tagged data elements with the requirements of the taxonomy being used.

Finally, auditors need to examine whether there is an approval process in place that describes how financial statements should be created from tagged data for inclusion on Web sites or for other purposes. These procedures should be applied to business reports generated at any point in time and should be required for any report updates. For reports generated on a real-time basis, the organization should implement a more complex set of procedures that ensure the integrity and accuracy of changes to tagged data on an ongoing basis.

Assurance Issues

Where assurance is concerned, auditors need to pay close attention to the different issues that might impact XBRL use and its effectiveness. "Auditors should use multiple validation tools, to ascertain the quality of the data in the XBRL report and not just rely on the preparer's tool for validation assurance," explains Mueller. "This is because different tools have slightly different approaches for tagging business reports with XBRL tags and preparers might have their own built-in validation processes, which may not be as rigorous as the tests conducted by other users." As a result, testing the validity of the tags with another validation tool is a good practice when auditing XBRL business report filings. "This second opinion can flush out any issues concerning the improper use of tags, conflicting contexts, improper extension of base taxonomies, or just missing information," adds Mueller.

Different assurance issues auditors need to pay close attention to include:

- **Reviewing policies and procedures that describe how XBRL statements are generated at a point in time.** To make sure these policies and procedures are effective, auditors need to review the controls that oversee the use of an appropriate taxonomy, the tagging of data, and the integrity of tagged data. Auditors also need to document and test these controls for their effectiveness and determine if the appropriate taxonomy is used when generating the statement. Finally, auditors need to test the data tagging procedure to determine if it is appropriate and includes all the data required.
- **Reviewing procedures that describe how statements are generated on a real-time basis.** When XBRL is used on a real-time basis, additional controls may be needed to ensure the integrity and accuracy of the tagged data. As a result, auditors need to identify and evaluate these controls. Furthermore, any online monitoring and exception reporting software used by the organization also can be used for assurance purposes. For instance, continuous audit procedures can be developed to flag conditions based on the most appropriate exception reports, such as unauthorized

changes in selected data elements, while other audit software can be used to monitor selected conditions and generate periodic reports at random intervals for audit activities.

As stated earlier, picking the right taxonomy is one of the most important issues auditors need to pay close attention to — if the right taxonomy is not picked, the auditor may be unaware there is an error in the reported data. To verify whether XBRL documents conform to applicable XBRL taxonomies and specifications, the American Institute of Certified Public Accountants and Public Company Accounting Oversight Board recommend that organizations render the report. (See *Attest Engagements Regarding XBRL Financial Information Furnished Under the XBRL Voluntary Financial Reporting Program on the Edgar System* [PDF, 59 KB]).

"Rendering means to convert the XBRL tags into human-readable form, such as PDFs or printable documents," explains Mueller. Therefore, if somebody gives the auditor a financial statement in an Excel spreadsheet, the auditor would convert the spreadsheet into XBRL and run the data through another program that takes the tags used as part of the chosen taxonomy and puts them back into human-readable form. The auditor would then print the original Excel spreadsheet and the final report from the second application and compare them side by side. If there is a problem with the taxonomy chosen, it will show in the form of missing data. "Another method of reviewing XBRL-tagged documents includes opening the XBRL report as a source-code document and testing the tags in the instance document," Mueller adds.

PROBLEMS WITH EXTENSION TAXONOMIES

In addition to the issues associated with choosing the wrong taxonomy discussed above, the use of extension taxonomies may pose additional issues when creating XBRL tags. An extension taxonomy is created by an organization or XBRL user to cover information that is not included in an approved or acknowledged taxonomy. For example, an XBRL user may start applying a taxonomy to a specific financial statement and discover there's a line item that's not covered by the taxonomy. The organization will then create its own specialized dictionary or extension taxonomy for those line items that are not in the main dictionary.

XBRL International recognizes two types of externally developed taxonomies – approved or acknowledged. Approved taxonomies have to comply with the official XBRL guidelines for that type of taxonomy as well as with XBRL Specifications, a technical explanation of what XBRL is and how it works. The current specification for XBRL is version 2.1, which can be found on XBRL International's Recommendations Web page. On the other hand, acknowledged taxonomies only have to comply with the XBRL Specifications. Other taxonomies include those used for financial, statistical, tax, and sustainability reporting, as well as the Global Ledger taxonomy, a special taxonomy that supports collation of data and internal reporting within organizations.

When it comes to extension taxonomies, auditors need to review whether the taxonomy was created and implemented correctly. In addition, users may think they need an extension taxonomy, when in fact the tags are already covered in an approved or acknowledged taxonomy. Consequently, they spend additional time creating an extension taxonomy that is not really needed, which increases the changes of introducing errors into the XBRL information supply chain.

OTHER ISSUES

Additional issues auditors need to keep in mind include those pertaining to internal controls and risk assessments, as well as problems validating and checking taxonomies and instance documents. Following is a discussion of each.

Internal Controls

As XBRL becomes more integrated in the company's information supply chain, internal controls and their evaluation become more critical. Internal controls will need to be in place for:

- Creating, using, testing, and maintaining extension taxonomies.
- Mapping data to XBRL instance documents.
- Automating subsequent mappings.
- Performing change management activities related to all aspects of XBRL.

Consequently, internal auditors need to determine whether internal controls are documented properly and collect evidence to test those controls. Before this is done, the internal audit department should create an XBRL audit team to develop a technical understanding of XBRL and prepare an appropriate audit plan.

Auditors need to keep in mind that the XBRL instance document will influence the types of controls that need to be in place. For example, appropriate internal controls should be integrated as part of the XBRL instance document, when creating extension taxonomies, and when testing and maintaining a taxonomy's processes and procedures. If errors are accidentally injected into the XBRL instance document, or a perpetrator purposely makes changes to commit fraud, internal decisions based on those XBRL instance documents will be distorted.

Risk Assessments

From a risk assessment perspective, XBRL risks can be divided in four categories:

1. Technology risks.
2. Mapping errors.
3. Fraud risks.
4. External risks.

When examining technology risks, auditors need to determine whether XBRL is being used correctly and whether extension taxonomies are created and implemented correctly. Auditors also need to determine if extension taxonomies and instance documents were reviewed for their quality. One way to do this is by performing a round trip, a process in which the resulting XBRL instance document is rendered into human-readable text. Round tripping enables the auditor to compare the original document to the rendered document line-by-line to determine if the rendered document is a faithful representation of the original document.

The second kind of risk is related to mapping errors. For example, was the financial statement account mapped to the correct XBRL tag? Answering this question can help internal auditors determine whether the XBRL user who created the instance document made a judgment error (i.e., selecting an inappropriate XBRL tag) or a mechanical error (i.e., inadvertently mapping a concept to the wrong tag). Furthermore, because mapping risks are increased when the XBRL data is created in real time, the auditor may not be able to review the XBRL output. Therefore, algorithms used to tag the XBRL data need to be evaluated during the risk assessment.

The use of real-time reporting also will enable auditors to use continuous auditing. As a result, real-time reporting of XBRL data will not only affect the organization, but the use of continuous audit techniques as well. "Auditors who wish to use XBRL as a way to facilitate continuous auditing should consider becoming acquainted with XBRL by experimenting with it," Hoffman comments. "Build a prototype and try XBRL out. Prototypes are a great way to learn."

Fraud represents a third area of risk. A major question auditors need to ask is whether the XBRL instance document was used to commit fraud. The relative level of fraud risks depends on where XBRL is being used in the information supply chain. For instance, at the end of the supply chain (e.g., when supplying an instance document to the U.S. Securities and Exchange Commission [SEC.]), XBRL fraud risk is probably low. This is because perpetrators know it is relatively easy for anybody to compare the official filling with the XBRL instance document and uncover any differences. On the other hand, the risks associated with XBRL instance documents increase when XBRL is used internally by the organization because there may be no paper trails to compare instance documents, which also may not be reviewed by an independent third party (e.g., an external auditor).

Finally, internal auditors need to be on the lookout for any external risks that might affect the accuracy of XBRL-generated reports. A major external risk includes hacking attempts or vulnerabilities. For instance, because XBRL documents may include internal and external links to the organization, hackers may try to change those links or the linked files. This would enable the hacker to view the source code of an XBRL instance document, identify the names and locations of extension taxonomies, and make changes to the instance document or extension taxonomy. To decrease hacking attempts, auditors need to recommend that organizations have the appropriate firewall encryptions in place and that all firewall security controls are tested for their effectiveness.

A second source of external risks is the inappropriate reliance on XBRL documents. When an XBRL document is created, users may download the document directly into an analysis tool, ignoring the paper-based or other official documents that accompany the XBRL report. As a result, the report's consumer may not fully understand or be aware of any limitations that are part of the XBRL instance document, which was made available to the public. For example, the SEC allows companies to submit XBRL documents without their accompanying notes. Therefore, if someone downloads the XBRL document from a company's Web site or the SEC's EDGAR filing system, they may not fully understand all the information included in the report.

MOVING FORWARD

"XBRL can be used to overcome existing weaknesses in controls by improving the integration of data within an organization and to its auditors," Cohen explains. Although XBRL use carries its own audit and control implications, it "overcomes many of the issues and problems associated with the filing of paper-based reports and manual audit activities, such as manual entry and re-entry of information, and permits auditors to use centralized and standardized rules and tests," he adds. As a result, becoming acquainted with XBRL — its many benefits and control issues — is of special importance to internal auditors and organizations as countries worldwide start to mandate its use, including the SEC in the United States.

For additional information on the different audit and controls issues discussed in this article, auditors can refer to *XBRL: Potential Opportunities and Issues for Internal Auditors (2005),* published by The Insitute of Internal Auditors' Research Foundation.

About the Author

Glen Gray, Ph.D., CPA, s a professor in the Accounting and Information Systems Department at California State University at Northridge. He can be contacted at glen.gray@csun.edu

Originally published in ITAudit, Vol. 10, August 10, 2007, published by The Institute of Internal Auditors Inc., www.theiia.org/itaudit.

The Problem With Document Destruction

Organizations can overlook the importance of documents until things go wrong. Make sure document retention and destruction policies and procedures are being implemented before a disaster can occur.

CRAIG S. WRIGHT, MNSA, CCE, GCA
MANAGER OF INFORMATION SYSTEMS SYDNEY, AUSTRALIA

Sound business practices dictate that document management be a priority for most organizations. However, the primary focus of managing information for many organizations centres around securing financial information against theft or unintentional release. While this is certainly a critical component of document management, organizations need to remember that the more routine, day-to-day documents created by employees at all levels can be just as critical to the success or failure of the business. What organizations keep and what they destroy should be a well thought-out process and managed appropriately.

The importance of such materials is evidenced by the growing number of regulatory requirements targeted at non-financial information such as the Anti-terrorism, Crime and Security Act 2001 introduced by the UK government following the terrorist attack in New York on September 11, 2001. This act encourages service providers to follow a voluntary code of practice, where e-mail is held under a six-month retention period. Other cases where internal documents and e-mails have played an important role are with Enron, WorldCom, Parmalat, and Royal Ahold. Such requirements and court cases also illustrate the changing complexities of document management, which must address both hardcopy materials as well as electronic data.

Organizations often realize the true value of proper document management when things go wrong, and previously overlooked items take on great significance. Within the internal audit department, one such example is source documents, which should be handled with special care in case they are needed to trace how audit findings, data collection, or transactions were conducted. Oral testimony, without evidentiary support, is not reliable and in a court of law, may be considered inadmissible. What documents organizations keep and what they destroy can send either positive or negative messages when faced with a challenging legal situation.

DESTROYING DOCUMENTS: BAD FOR BUSINESS OR ILLEGAL

Putting the Pieces Together

Forensics accountants and other investigators use evidentiary fragments to reconstruct transactions. In the absence of supporting documentation, it is often necessary to reconstruct transactions and contracts. The parol evidence rule, however, precludes the introduction of ancillary evidence which contradicts a written contract. In the absence of the written contract, evidentiary fragments may be used. Because anything outside of a written contract is parol evidence (including testimony about what was said during the negotiations, proposals, or recordings of conversations), the failure to maintain the original records could result in a detrimental judgement. This judgement could be diametrically opposed to what was intended in the written contract.

Serious consideration should be given to the destruction of any document, and it should be noted that the destruction of documents in some cases is not just illegal but criminal. For instance, a company officer or director who destroys or falsifies a document affecting the company's property or affairs is liable to prosecution under the Australian Corporations Act 2001.

According to this law, if there is a suspicion of wrongdoing, individuals must prove that the destruction of documents was not done with the intention to deceive. In many cases, these are statutory strict liability offences. In other words, the prosecution only needs to prove the facts (i.e., that a defendant destroyed the documents). It is up to the defendant to disprove intent. This is not always easy to do in a court of law. In fact, according to section 1309 of the Australian Corporations Act 2001, it is an offence if an officer or employee fails to take reasonable steps to ensure the accuracy and protection of records.

In Victoria, Australia, recent changes to the Crimes Act 1958 have created "a new offense in relation to the destruction of a document or other thing that is, or is reasonably likely to be, required as evidence in a legal proceeding." This act, punishable by up to five years imprisonment, affects anyone who destroys or authorizes the destruction of any document that may be used in a legal proceeding (including potential future legal proceedings).

Under section 286(1) of the Corporations Act, a company must keep “written financial records that: correctly record and explain its transactions and financial position and performance; and would make true and fair financial statements able to be prepared and audited.”

If a dispute has previously arisen or is considered likely, it is hazardous to destroy any documents. Cases where provisions for litigation have been included in audit reports are a strong example. In instances where it is probable that a dispute may arise, or after a dispute has begun, a conscious choice to destroy documents could make one liable under the criminal offence of obstructing justice.

Leveraging Technology to Manage Document Retention

One way for organizations to manage their process is to leverage readily available advanced technologies, such as scanners to preserve files. Coupled with optical character recognition (OCR), scanned images can be stored both as an original copy for evidentiary purposes and as a tagged document with keywords for searching. Use of this technology minimizes the risk associated with paper records, especially when searching through paper documents within certain date ranges. Furthermore, scanned images can be dated and automatically marked for deletion at the end of their retention period.

Ask any forensic accountant; the existence of omitted documents is usually easy to trace because they are referred to in existing documents. If the case goes to court, it is necessary to list not only documents in one's possession, custody, or power but also those that once existed and have been destroyed.

The destruction of documents can adversely influence a case through inference, as demonstrated in the United Kingdom, Infabrics v. Jaytex. After the commencement of the case, it was discovered that most of the invoices, stock records, and similar documents had been destroyed. The judge stated that he was "not prepared to give the defendants the benefit of any doubt or to draw an inference in their favour where a document, if not destroyed, would have established the matter beyond doubt."

DOCUMENT MANAGEMENT CONSIDERATIONS

With the increasing requirements for electronic documents, companies should update their document retention policies. These policies should not be disorganized or ad hoc. In the past, there were definite limitations on how long files should be retained (with most professions keeping papers for at least seven years). However, recent decisions made by courts all over the world requiring organizations to keep records for a period after the final transaction, not from when the document was created, make establishing general guidelines more difficult.

Leading practices in the area of document management suggest that companies should adopt a document retention policy that ensures items are only discarded or destroyed in accordance with governing regulations and in a systematic manner. Developing a written policy on document destruction and retention, to be applied consistently, is a shrewd move on the part of any organization.

MINIMUM DOCUMENT RETENTION GUIDELINES

The minimum requirement for data retention varies widely across jurisdictions, countries, and oftentimes, business disciplines, as illustrated by some of the wide variations reflected in Figure 1.

Examples of Data Retention Requirements

Web activity data	4 days retention period
Basic Commercial Contracts	6 years after discharge or completion
Deeds	12 years after discharge
Land contracts	12 years after discharge
Product liability	A minimum of 10 years
Patent deeds	20 years
Trademarks	Life of trademark plus 6 years
Copyright	50 years after author's death

Figure 1

APPLICATIONS TO INTERNAL AUDIT

Document management is not an issue confined to Australia and the UK. Rather, it is an ever-growing concern for organizations throughout the world. In particular, the increasing use and complexity of document management systems and databases is driving an invigorated need to implement effective controls. It is no longer enough for the internal IT auditor to rely on an isolated snapshot of the system. It is essential that an understanding of document retention requirements based on jurisdictional specifications be maintained.

International Organizations for Standards (ISO) Guidance on Document Retention 27001

ISO requirement 27001 states that records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the information security management system (ISMS). They shall be protected and controlled. The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations. Records shall remain legible, readily identifiable, and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time, and disposition of records shall be documented and implemented."

There are a number of steps that internal auditors can use to aid in auditing electronic documents. By incorporating controls into databases and other systems, the audit staff are able to ensure that legislative requirements are being met. Some steps that may be undertaken include:

- **Classifying all documents that are scanned or electronically created using systems of automated controls and allocations.** Electronic records management systems are becoming more commonly used for this task as they can automate the allocation of documents to a classification that best reflects the material they contain.
- **Using digital analysis techniques and data mining to search through system storage and data warehouses for keywords and classifications.** The rise of data warehousing has led to the ability to configure automated searches for data that has been incorrectly classified or is past its retention period using text mining.
- **Configuring key fields in databases and making rules to create isolated copies of required documents.** By configuring a centralized store of documents, key document recovery is a more efficient process. Many banks and credit unions have implemented processes that centralize and manage transaction confirmations, retirement information, loan applications, and even meeting notes or minutes.
- **Implementing formal policies and procedures.** International

Organization for Standards 27001, and 15489 (Information and Documentation – Records Management) and the Model Requirements for Management of Electronic Records provide guidelines for data retention.

- **Using network scanning for defined against classifications**. An intrusion detection system may be configured to alert on key phrases and data sent on unauthorized streams (i.e., using unencrypted e-mails). Databases may be tested to ensure that sensitive data is only retained in secured tables.

GOING FORWARD

Organizations and their internal audit departments need to stay vigilant in their oversight of the document management process, paying special attention to items that seem to get lower levels of attention than financial data. Also, it is wise for organizations to remember that e-mail has become a common means to distribute board minutes, reports, and other sensitive data. As such, the need to define data retention strategies has only increased. So don't wait until the next time your organization decides to purge files, e-mails, or other miscellaneous electronic documents — make sure document retention and destruction policies and procedures are being implemented before a disaster can occur. Remember, there is much more to document retention than managing disk space.

Craig Wright is a manager of information systems in Sydney, Australia. He is currently working on his tenth academic degree! He can be contacted at Craig.Wright@bdo.com.au

Originally published in ITAudit, Vol. 10, August 10, 2007, published by The Institute of Internal Auditors Inc., www.theiia.org/itaudit.

HUMOUR PAGES

NEW OFFICE POLICIES

Dress Code:

1) You are advised to come to work dressed according to your salary.

2) If we see you wearing Prada shoes and carrying a Gucci bag, we will assume you are doing well financially and therefore do not need a raise.

3) If you dress poorly, you need to learn to manage your money better, so that you may buy nicer clothes, and therefore you do not need a raise.

4) If you dress just right, you are right where you need to be and therefore you do not need a raise.

Sick Days:

We will no longer accept a doctor's statement as proof of sickness. If you are able to go to the doctor, you are able to come to work.

Personal Days:

Each employee will receive 104 personal days a year. They are called Saturdays & Sundays.

Bereavement Leave:

This is no excuse for missing work. There is nothing you can do for dead friends, relatives or co-workers. Every effort should be made to have non-employees attend the funeral arrangements in your place. In rare cases where employee involvement is necessary, the funeral should be scheduled in the late afternoon. We will be glad to allow you to work through your lunch hour and subsequently leave one hour early.

Bathroom Breaks:

Entirely too much time is being spent in the toilet. There is now a strict three-minute time limit in the stalls. At the end of three minutes, an alarm will sound, the toilet paper roll will retract, the stall door will open, and a picture will be taken. After your second offence, your picture will be posted on the wall in all the offices and the warehouse under the “Chronic Offenders” category. Anyone caught smiling in the picture will be sectioned under the company's mental health policy.

Lunch Break:

* Skinny people get 30 minutes for lunch, as they need to eat more, so that they can look healthy.

* Normal size people get 15 minutes for lunch to get a balanced meal to maintain their average figure.

* Chubby people get 5 minutes for lunch, because that's all the time needed to drink a Slim-Fast.

Thank you for your loyalty to our company. We are here to provide a positive employment experience. Therefore, all questions, comments, concerns, complaints, frustrations, irritations, aggravations, insinuations, allegations, accusations, contemplations, consternation and input should be directed elsewhere.

THINGS COMPUTERS CAN DO IN MOVIES

1. Word processors never display a cursor.
2. You never have to use the space-bar when typing long sentences.
3. Movie characters never make typing mistakes.
4. All monitors display inch-high letters.
5. High-tech computers, such as those used by NASA, the CIA or some such governmental institution, will have easy to understand graphical interfaces.
6. Those that don't have graphical interfaces will have incredibly powerful text-based command shells that can correctly understand and execute commands typed in plain English.
7. Note: Command line interfaces will give you access to any information you want by simply typing, “ACCESS THE SECRET FILES” on any near-by keyboard.
8. You can also infect a computer with a destructive virus by simply typing “UPLOAD VIRUS”. (See “Fortress”.)
9. All computers are connected. You can access the information on the villain's desktop computer even if it's turned off.
10. Powerful computers beep whenever you press a key or the screen changes. Some computers also slow down the output on the screen so that it doesn't go faster than you can read. (Really advanced computers will also emulate the sound of a dot-matrix printer.)
11. All computer panels operate on thousands of volts and have explosive devices underneath their surface. Malfunctions are indicated by a bright flash of light, a puff of smoke, a shower of sparks and an explosion that causes you to jump backwards.
12. People typing on a computer can safely turn it off without saving the data.
13. A hacker is always able to break into the most sensitive computer in the world by guessing the secret password in two tries.
14. You may bypass “PERMISSION DENIED” message by using the “OVERRIDE” function. (See “Demolition Man”.)
15. Computers only take 2 seconds to boot up instead of the average 2 minutes for desktop PCs and 30 minutes or more for larger systems that can run 24 hours, 365 days a year without a reset.
16. Complex calculations and loading of huge amounts of data will be accomplished in under three seconds. Movie modems usually appear to transmit data at the speed of 100 gigabytes per second.
17. When the power plant/missile site/main computer overheats, all control panels will explode shortly before the entire building destructs.
18. If you display a file on the screen and someone deletes the file, it also disappears from the screen (See “Clear and Present Danger”).
19. If a disk contains encrypted files, you are automatically

asked for a password when you insert it.

20. Computers can interface with any other computer regardless of the manufacturer, or galaxy, where it originated. (See “Independence Day”.)
21. Computer disks will work on any computer that has a floppy drive and all software is usable on any platforms.
22. The more high-tech the equipment, the more buttons it will have. (See “Aliens”.)
23. Note: You must be highly trained to operate high-tech computers because the buttons have no labels except for the “SELF-DESTRUCT” button.
24. Most computers, no matter how small, have reality-defying three-dimensional active animation, photo-realistic graphics capabilities.
25. Laptops always have amazing real-time video phone capabilities and performance similar to a CRAY Supercomputer.
26. Whenever a character looks at a monitor, the image is so bright that it projects itself onto their face. (See “Alien” or “2001”.)
27. Searches on the internet will always return what you are looking for no matter how vague your keywords are. (See “Mission Impossible”, Tom Cruise searches with keywords like “file” and “computer” and 3 results are returned.)

THE GREAT WRITER

There was once a young man who, in his youth, professed his desire to become a great writer.

When asked to define “great” he said, “I want to write stuff that the whole world will read, stuff that people will react to on a truly emotional level. Stuff that will make them scream, cry, and howl in pain and anger!”

He now works for Microsoft, writing error messages.

HELP DESK?

It's backup day today so I'm bored, however, does have it's advantages. I assign the tape device to null – it's so much more economical on my time as I don't have to keep getting up to change tapes every 5 minutes. And it speeds up backups too, so it can't be all bad.

A user rings

“Do you know why the system is slow?” they ask

“It's probably something to do with...” I look up today's excuse “.. clock speed”

“Oh” (Not knowing what I'm talking about, they're satisfied) “Do you know when it will be fixed?”

“Fixed? There's 275 users on your machine, and one of them is you. Don't be so selfish - logout now and give someone else a chance!”

“But my research results are due in tomorrow and all I need is one page of Laser Print..”

“SURE YOU DO. Well; You just keep telling yourself that buddy!” I hang up.

Sheesh, you'd really think people would learn not to call!

The phone rings. It'll be him again, I know. That annoys me. I put on a gruff voice

“HELLO, SALARIES!”

“Oh, I'm sorry, I've got the wrong number”

“YEAH? Well what's your name buddy? Do you know WASTED phone calls cost money? DO YOU? I've got a good mind to subtract your wasted time, my wasted time, and the cost of this call from your weekly wages! IN FACT I WILL! By the time I've finished with you, YOU'LL OWE US money! WHAT'S YOUR NAME - AND DON'T LIE, WE'VE GOT CALLER ID!”

I hear the phone drop and the sound of running feet - he's obviously going to try and get an alibi by being at the Dean's office. I look up his username and find his department. I ring the Dean's secretary.

“Hello?” she answers

“Hi, SIMONE, HELP DESK HERE, LISTEN, WHEN THAT GUY COMES RUNNING INTO YOUR OFFICE IN ABOUT 10 SECONDS, CAN YOU GIVE HIM A MESSAGE?”

“I think so...” she says

“TELL HIM `HE CAN RUN, BUT HE CAN'T HIDE'”

“Um. Ok”

“AND DON'T FORGET NOW, I WOULDN'T WANT TO HAVE TO TELL ANYONE ABOUT THAT FILE IN YOUR ACCOUNT WITH YOUR ANSWERS TO THE PURITY TEST IN IT...”

I hear her scrabbling at the terminal...

“DON'T BOTHER – I HAVE A COPY. BE A GOOD GIRL AND PASS THE MESSAGE ON”

She sobs her assent and I hang up. And the worst thing is, I was just guessing about the purity test thing. I grab a quick copy anyway, it might make for some good late-night reading.

Meantime backups have finished in record time, 2.03 seconds. Modern technology is wonderful, isn't it?

Another user rings.

“I need more space” he says

“Well, why don't you move to Texas?” I ask

“No, on my account, stupid.”

Stupid?!?.... Uh-Oh..

“I'm terribly sorry” I say, in a polite manner equal to that of Jimmy Stewart in a family Matinee “I didn't quite catch that. What was it that you said?”

I smell the fear coming down the line at me, but it's too late, he's a goner and he knows it.

“Um, I said what I wanted was more space on my account, *please*”

“Sure, hang on”

I hear him gasp his relief even though he covered the mouthpeice.

“There, you've got plenty of space now”

“How much have I got”

Now this REALLY ANNOYS ME! Not only do they want me to give them extra disk, they want to check it, to correct me if I don't give them enough. They should be happy with what I give them *and that's it*!!!

Back into Jimmy Stewart mode.

“Well, let's see, you have 4 Meg available”

“Wow! Eight Meg in total, thanks!” he says pleased with his bargaining power

“No” I interrupt, savouring this like a fine red, at room temperature “4 Meg in total...”

“Huh?... I'd used 4 Meg already, How could I have 4 Meg available?”

I say nothing ………………… it will come to him!!

The following is an email that I received recently informing me that I had won a prize ………… Ed.

FROM THE DESK OF THE DIRECTOR INTERNATIONAL WORLDWIDE INTERNET USER LOTTERY PRIZE AWARD DEPT.

Dear Internet User,

YOUR WINNING NOTIFICATION FOR USING THE INTERNET.

I am pleased to inform you that one of the best things that can happen to any Internet user is to be rewarded for spending money and time on the Internet. You may not have known that over one hundred billion people daily surf the Internet on regular basis for one reason or other. These Internet users including yourself, pay access fees to various Internet Service Providers (ISP) all over the world who in turn remit surplus funds to the numerous World Wide Internet Technology Companies (WWITC) for the development and advancement of Global Information Technology.

So much money is generated from people like you all over the World for using the Information Superhighway (the Internet) without your being aware the enormous sum that go to the stake holders (WWWITC). Without your patronage, this would not have been possible. After we conducted a research on the issue, we concluded that Internet users should be compensated. As a result, we embarked on a worldwide lottery promotion with a sophisticated automated database to randomly select E-mail accounts that frequently surf the Internet. Consequent upon this, your E-mail address was picked for Category Winners.

After the automated computer ballot, your E-mail address emerged as a winner in the category “A” with the following numbers attached

Ref Number: PW EH 9590 OG 0612,

Batch Number: PA 563881545-NL/2007

You and other category winners are therefore to receive a cash prize of Five Million United States Dollars ($5,000,000.00) respectively from the total payout of One Billion US Dollars earmarked in the lottery for category winners. Your prize award has been insured with your E-mail address, which qualified you for the lottery and will be transferred to you upon meeting our requirements, statutory obligations, verifications, validations and satisfactory proof of E-mail address ownership.

To file in for the processing of your money, you are advised to contact our certified and accredited claims agent for category “A” winners with the information below:

CLAIMS AGENT.

Name: Pierce Van Barsel

Phone: +316-169-41206

Email: s_claimsofficer@yahoo.com

You will provide him with the following information:

First name:

Last Name:

Telephone/Fax number:

Nationality:

Age:

Occupation:

NOTE: All winnings must be claimed not later than 14 days, thereafter unclaimed funds would be forfeited after a trio repeated forwarding of this message to you without your response. Remember to quote your reference information in all correspondence. (Ref No: PW EH 9590 OG 0612, Batch No: PA 563881545-NL/2007),

You are to keep all lotto information confidential, especially your reference numbers and the password of your E-mail address. Since we do not know you, if an impostor hacks your E-mail account ID and claims your money without our knowledge, we shall not be liable. Double claims will not be entertained so be careful. Furthermore, should there be any change of address do inform our agent as soon as possible.

Congratulations! Thank you for being a user of the World Wide Web.

Yours Faithfully,
Marry Jones
Lottery Coordinator.
Thank you and congratulations!!!

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

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	Ross Palmer	chair.irma@bcs.org.uk
SECRETARY	Siobhan Tracey	Siobhan.Tracey@dsgiplc.com
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Adam Carden	adam.carden@scottish-southern.co.uk
JOURNAL EDITOR	John Mitchell	john@lhscontrol.com
WEBMASTER	Allan Boardman	allan@internetworking4u.co.uk
EVENTS PROGRAMME CONSULTANT	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON – IIA & NHS	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON – ISACA	John Mitchell	john@lhscontrol.com
MARKETING	Vacant	
ACADEMIC RELATIONS	George Allan	george.allan@port.ac.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**
	Userid = irmamembers
	Password = 4members07
		Members' area

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)

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

INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)* For details of BCS membership visit www.bcs.org	£25
INDIVIDUAL MEMBERSHIP *(A members of the BCS)* BCS membership number: ___________________________	FREE
STUDENT MEMBERSHIP – Full-time only and must be supported by a letter from the educational establishment. *(An annual quota is in operation, so IRMA retains the right to close this level of membership at any time).* Educational Establishment: ___________________________	FREE

Please circle the appropriate subscription amount and complete the details below.
All communications from the Group are likely to be electronic.
Please tick this box to indicate you agree to be contacted this way. □

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

BCS IRMA SPECIALIST GROUP ADVERTISING RATES

Reach the top professionals in the field of Information Risk Management and Audit 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 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

Direct e-mailing

We can undertake direct e-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 of £350.

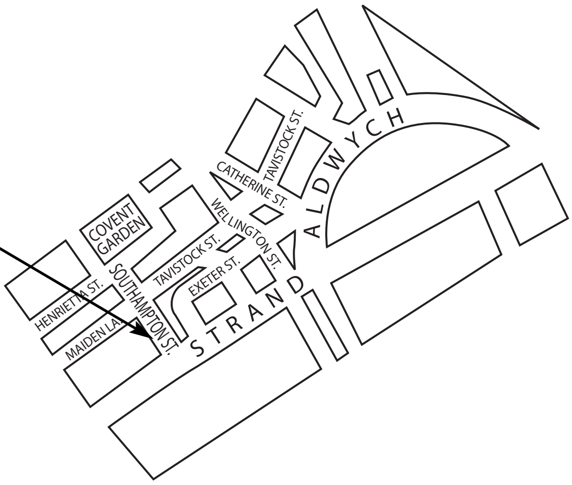
Contact

Administration

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

Meeting Venue unless otherwise stated

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


TAVISTOCK ST.
CATHERINE ST.
WELLINGTON ST.
ALDWYCH
COVENT GARDEN
TAVISTOCK ST.
EXETER ST.
HENRIETTA ST.
SOUTHAMPTON ST.
MAIDEN LA.
STRAND