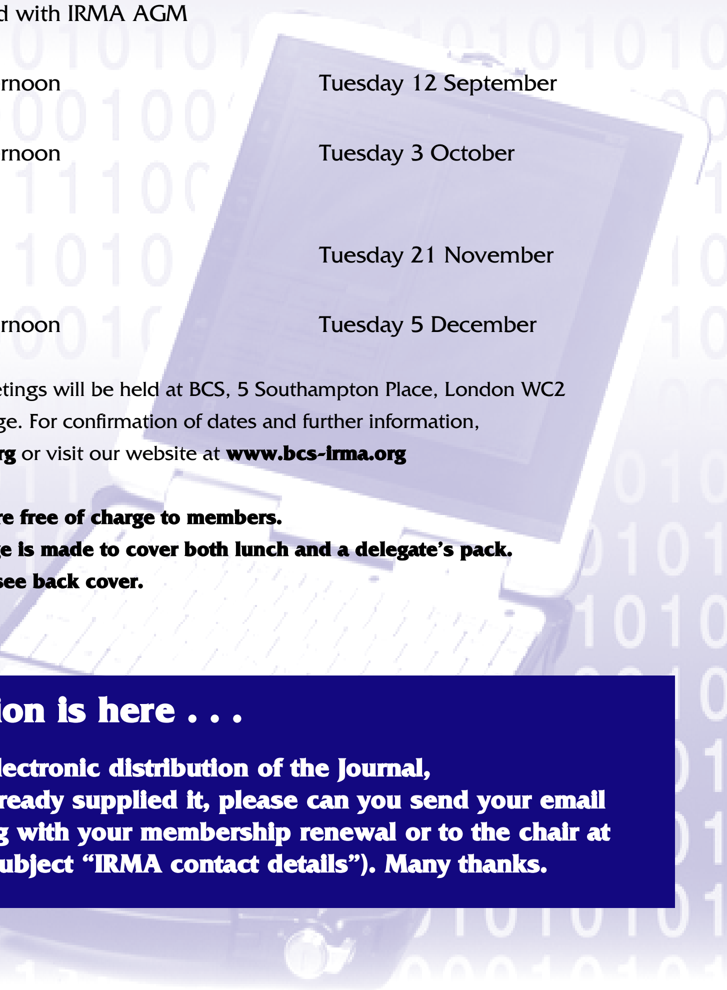
IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

JOURNAL
volume 16 number 3 autumn 2006 ISSN 1741-4229

Programme of Briefings & Meetings 2006

Title	Meeting type	Date
Computer Audit Basics 4: Application Controls	Late afternoon meeting	Tuesday 24 January
Control Aspects of ITIL (Service Delivery) / Cobit	Late afternoon meeting	Tuesday 07 February
Wireless Technology	Late afternoon meeting	Tuesday 07 March
Latest Developments in IT Law	Late afternoon meeting combined with IRMA AGM	Tuesday 02 May
Spreadsheet Risks: Ubiquity, Severity & Legality?	Late Afternoon	Tuesday 12 September
Lifting the lid on Stolen Laptops	Late Afternoon	Tuesday 3 October
Project control: the auditor's role in IS projects and systems development – joint meeting with ICAEW	Full Day	Tuesday 21 November
TBA	Late Afternoon	Tuesday 5 December



Apart from any joint meetings with other organizations all meetings will be held at BCS, 5 Southampton Place, London WC2
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 with your membership renewal or to the chair at brewer.alex@gmail.com (preferably with the subject "IRMA contact details"). 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.

Editorial Panel

Editor
John Mitchell
LHS Business Control
Tel: 01707 851454
Fax: 01707 851455
Email: john@lhscontrol.com

Academic Editor
Dr George Allan
University of Portsmouth
Tel: 023 9284 6425
Fax: 023 9284 6402
email: george.allan@port.ac.uk

Phil Kelly
Liverpool John Moores University
Tel: 0151 231 3838
Email: p.kelly1@ljmu.ac.uk

BCS Matters
T.B.A.

Events Reporter
Rupert Kendrick
Tel/Fax: 01234 782810
Email: RupertKendrick@aol.com

Australian Correspondent
Bob Ashton
Wide Bay Australia Ltd
Tel: +61 7 4153 7709
bob_ashton@excite.com

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

Produced by Carliam Artwork,
Potters Bar, Herts

Editorial

John Mitchel

All that stands between your specialist group and its winding up are the activities of the volunteers on its Management Committee. Alex Brewer, our Chairman has resigned for reasons he explains in his column and I know that two other members, Raghu Iyer and Wal Robertson are intending to resign at the end of their stint this year. Jean Morgan stepped in as pro-tem Chairman to keep things going and Ross Palmer will now be taking the lead until next year's AGM. Things are looking a little grim as we become too thinly stretched to deliver an adequate service to you. We really do need volunteers to help out, especially in the area of forthcoming events. Come on, don't be shy. Put back in what you may have previously taken out. Contact Ross and volunteer. He can be contacted at ross.palmer@hrplc.co.uk. What's in it for you? If you need to ask, then perhaps you shouldn't volunteer. However, you get free attendance at our chargeable events and first refusal on a places that we are often offered at other conferences.

Moving on to an area of national, rather than parochial importance, the recent fire at Kings Cross which stopped north/south trains into London leads me to query the resilience of our national infrastructure. In fact, it wasn't the fire that stopped the trains from running, but the need to evacuate a nearby signal box. Now, if you needed to evacuate your data centre I suspect the powers that be would be pretty upset if your BCP was unable to deliver an adequate service. But this is exactly what happened with Network Rail. After all, this was only an interruption and it brought travel chaos. What would have happened if the signal box itself had been totally destroyed? So, I start tracking down who should be asking the awkward questions. First to NISCC (National Infrastructure Security Co-ordination Centre) where the Deputy Director informs me that it is not their bailiwick. "No, we deal with electronic security, not hardware". "But surely the signalling stuff is electronic". "Sorry, ask the Department of Transport". So I email the Secretary of State for Transport. Now the Right Honourable Douglas Alexander MP must be a very busy man (or perhaps stuck on a train), because neither he nor his minions cared to respond. After several attempts I emailed Tony Blair with a query as to what exactly I have to do to get a response from his Secretary for State? Hey presto, I get an email from a minion who says that the signal failure is a Network Rail problem! Doooh! "No, Secretary of State, the national transport infrastructure is your responsibility". You and not me should be asking why Network Rail does not have an adequate BCP. So get out of your car and raise merry hell with them.

Which brings me to another area where I believe that we are being failed by the people we pay to run the country. The recent CPS report on its investigation into the death of Jean Charles de Menezes at the hands of a police firearms unit noted that "a log book of events was submitted for forensic examination to see if it had been altered and, if so, by whom. Two experts examined the relevant passage but they could not agree to the required standard whether there had been an alteration or, if there had been one, who may have done it. This meant there could be no prosecution of any individual in relation to the log book". Ignoring for the moment the bizarre use of Health & Safety legislation in the case of someone who was shot to death, the altering of a log book is a clear indication that police officers are not above committing a serious criminal offence. The Crown Prosecution Service may not have sufficient evidence to proceed with a case, but the fact remains that an official record may have been tampered with. At best this is forgery and at worse a conspiracy to pervert the course of justice, instigated by the very people responsible for upholding the law. The Police Complaints Commission and the CPS should be ashamed that they cannot effectively investigate a crime committed in their own back yard. What is wrong in using three experts and then taking the majority view? That's the way the Space Shuttle's computers are designed.

Academic integrity, or lack of it, has been aired in this column previously, but I was reminded on it again when I received a call for papers for a security symposium. It all looked fine until I got to the submission requirements. "For an accepted submission to be included in the proceedings and scheduled for presentation at the symposium: (1) a final version that responds to reviewers' comments and conforms to the specified format must be submitted by the final-version deadline, and (2) at least one of the authors must register to the symposium by the early-registration deadline". Requirement (2) is the killer. If you want your paper to be considered for publication you have to agree to pay to attend the conference. So you may have an excellent paper, but if you can't afford to fly to Spain, stay at a hotel and pay the conference fee, then tough luck, it doesn't even get considered. This means that money talks louder than academic integrity. Come along you academics. Make a stand and stamp out this unethical behaviour.

Finally, big brother is watching you as you travel around the London Transport system. If you have registered for an Oyster card, or have topped one up with your credit card, then they know who you are and where you have been. I noticed that the application form for the Oyster card does not follow the guidelines for Data Protection in that you cannot opt out from them contacting you for "administration, customer service & research". Secondly, their contacting you about "related products or services" is a default "opt in" when it should be a default "opt out". No response from TfL yet on my queries on this (well, it's only been a month), but another researcher was more successful regarding the number of times that information has been disclosed to the police. "Between August 2004 and March 2006 TfL's Information Access and Compliance Team received 436 requests from the police for Oyster card information. Of these, 409 requests were granted and the data was released to the police. Please note that before September 2005, some requests may have been received and answered without detailed statistical information being recorded". The researcher then asked how many of these requests were as a result of a court order. The answer was none. So my advice is to buy your Oyster card from a retailer and pay cash.

In this edition I welcome Brian Runicman who has taken over the "BCS Matters!" column from Colin Thomson. Mark Smith has provided his usual helpful list of members' benefits which shows the value for money you receive from your membership subscription. Alan Calder and Steve Watkins bring us up to date on ISO 27001, while David Cuthbertson suggests some quick wins for IT Management Teams. Not forgetting Bob Ashton from Australia who reports on the training situation down under.

Don't forget to volunteer for the Management Committee.

IRMA MEMBERS' BENEFITS DISCOUNTS

Mark Smith

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 2006 (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)
Websec 2006 (www.mistieurope.com)	15%	Lisa Davies (LDavies@mistiemea.com)

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.

Chairman's Corner

Alex Brewer

Just when you thought it was safe...

So here I am, waltzing through life, IRMA is starting to bloom again, events are starting to organize themselves, the committee seem content with life. So what could possibly go wrong? What might shake this?

Without going into the (not gory, but uncomfortable) details, other areas of my life are demanding attention to the extent that IRMA has fallen far down the list of priorities. Even in this state I realised that I could not continue without hurting the group, and faced with things that require sorting out (November's day, membership reminders), I did what I hope is the right thing, and said 'help' to the committee.

It was only a matter of time before my lack of focus affected the group badly in some way, so I felt I had to resign as Chair with immediate effect. I am fortunate that I have always liked the committee, both individually and as a group, but never imagined that I might have to call in a huge favour: doing this, and talking about it, does not come easily to me.

I must give thanks to the entire IRMA committee for stepping in and taking the load from me. Jean Morgan, our Treasurer, has stepped in as an interim only chair, and deserves a medal for taking that on.

So in a sense, this really does involve you, dear reader: the committee needs you more than ever, as I have to leave and concentrate on matters close to my heart. Please consider helping out – the specialist group is an interesting place, and the committee are good people, as I have found out directly.

In summary, focus on the things that really matter to you. In my case, that means relinquishing IRMA to focus on other, more important matters. Before I go, a last chance to air my obsessions with you...

RFID – more magic numbers

More magic numbers are appearing around us, measuring our lives even as we speak. The latest ones can be found in RFID tags the size of rice grains, which can carry up to 4 megabytes of data as well as an antenna to communicate with.

So let's go forward five to ten years and all of our clothes will have these devices embedded for the clothes retailer's stock control system. An RFID reader can capture all of the clothes a person wears as they pass it, and there is a very good chance that the association of the clothes RFID numbers will be a good way in which to track an individual (especially if I'm wearing my wife's lycra pants!). Does this constitute personal data? An individual can be found and tracked going through any shop checkout.

Will companies use this rich source of data? You be the judge.

RFIDs – access card readers

RFIDs are also just beginning to be problematic when it comes to getting into the office. This is because they are the core of card access systems to get into larger company offices or restricted areas of offices. The model of many card access systems is:

1. reader beams card to get its magic number
2. reader opens if the number is right.

The problem arises when someone builds a card reader that you can carry with you, one that can replay the magic numbers from other cards. So how do you know that the access you grant is only used by authorised staff?

If you have any doubts as to whether this is an issue do have a look at the Wired website – looking for 'RFID Hacking'. (Or the following link may still work: http://www.wired.com/wired /archive/14.05/rfid.html)

The nature of the problem looks very similar to the first generation of UK mobile phones which could be 'cloned'. So access control systems, long relied upon to keep business premises secure, may be at risk.

Lights on service

When the power fails, this has a direct economic impact in the UK. Some of you may remember the miners' strikes in the 1970s – which had an impact on the economy, and that in the days before computers were so pervasive in our lives.

Environmentalists have been going on about saving energy for years, however the consumption of energy (how many of you have those huge 4x4 cars?) keeps on rising.

The global environment concerning energy supplies is changing rapidly.

If you have followed the news, you will have noticed the sudden prominence of new companies on the international energy markets.

- Add to that the current madness in Gaza and Lebanon.
- Add to that the US taking Iran to task over NPT (even though they are in compliance).
- Add to that the sudden resurgence of UK nuclear power and the running out of North Sea oil and gas reserves.
- Add to that the dramatic increase in energy consumption in China and India

– Add to that the complications that privatisation brings when the system is run for profit rather than a critical infrastructure – aka the California experience. Also consider that the August 2003 power failure in London was partially caused by cost cutting on essential maintenance, a fact that only became apparent after a whistle-blower spilled the beans.

The above is a recipe for volatility in energy supplies not seen for many years. So one of the emerging challenges for us will be to consider the environment in which our businesses operate to see if they can simply provide a 'lights on' service.

OpenOffice (OO)

If you haven't seen OO and haven't got around to paying your Microsoft Office tax, I would recommend going to www.openoffice.org and considering downloading an excellent office package. I use it all of the time, and my daughters have stopped complaining because we don't have Word – OO allows you to open and save files in Office formats, but without having to use, and pay for, 'other Office products'.

Happy New IRMA Year

You should have your membership renewal – please send Janet the money promptly, and don't forget to make sure that your email address is current.

As ever, if you have any thoughts on the format or the content of the newsletter, or would like to submit a paper, please contact IRMA's administration at admin@bcs-irma.org.

And finally to reiterate, please do consider helping the committee. We meet at the lovely BCS London HQ. Benefits include free attendance at all IRMA events, and participation in ongoing BCS activity (such as an earlier consultation on ID cards). Expenses are available for attending committee meetings.

I wish you all the best. Please wish me luck.

Editor's Note. I am delighted to announce that since Alex penned this Ross Palmer has stepped in as Chairman until next year's AGM.

BCS Matters!

BRIAN RUNCIMAN, BCS Managing Editor, looks at a new programme to be launched by the Security Forum …

From phishing to cybercrime to forensics and more

Security – information security and IT security – is the biggest subject for ongoing debate in IT and BCS are addressing it head-on.

The BCS Security Forum is putting together a programme to look at current and forthcoming security subjects.

BCS already has two specialist groups working in this area – the Information Security Specialist Group and the Information Risk Management and Audit Group – but under the aegis of the Security Forum we are now widening our coverage. There will be a major event in January looking at business continuity and resilience. A monthly version of the electronic newsletter eBCS specifically for security issues is being launched in August and a new quarterly virtual magazine will follow in October.

A new look website dedicated to security will be the centre of the community, bringing together security experts, IT professionals, many of whom have a vested interest in the subject, and even providing advice for the public.

Security is already a subject well represented by the BCS with position statements, thought leadership debates and editorial content on the website, but we want to expand this even more. Recent additions to the content section are a report on the certainty of security breachs from David Thomas – deputy assistant director, FBI Cyberdivision – who presented on the subject to the World Wide Web Conference in Edinburgh. A report from the Infosecurity Europe 2006 keynote seminar discussing five things to go away and do to secure the future of your business is now online, as is a recent piece on risk management in the public sector

Other suggestions from members on what they would find useful are welcome and anyone interested in writing for us on the many subject areas involved in security should email editor@bcs.org.

The latest Thought Leadership debate was on a major security area: Critical National Information Infrastructure, who owns it and how do we protect it? A report is online now at www.bcs.org/thoughtleadership/cnii

The new website will be at www.bcs.org/security and will include strategy articles, reader offers, opinion pieces and more.

Brian can be contacted at **editor@bcs.org**

The Down Under Column

Bob Ashton – IRMA Oceania Correspondent

Conferences and Training

The ISACA CACS International Conference was held in Adelaide at the end of July. An entire stream was devoted to risk management, and was very well received. A significant characteristic of this conference was that none of the sessions specifically addressed the mechanics of IS auditing, although some aspects were addressed in pre and post conference workshops. This approach was deliberate on the part of the conference organizers, although it seemed unusual to some Australians who were used to seeing basic IS auditing skills presented at ISACA conferences. In North America in particular ISACA provides abundant opportunities in basic IS audit training through Training Weeks, Chapter Seminars and the Professional Seminar Series, and so it is not considered appropriate to be included in the agenda for the International Conference.

Most Australian centers do not seem to be as well served, however. There is always a demand for the education of IS auditors on how to perform their daily tasks, including basics such as how to perform an audit of Unix, Linux or Windows Server, or of ubiquitous applications such as SAP. Nature abhors a vacuum however, and this space is being filled in some Australian centres by the Institute of Internal Auditors, which is providing courses aimed at teaching IS auditing and deserves to be congratulated for it.

The ISACA Australian chapters' seeming lack of attention to promoting training in the basics seems odd given the resources available to them. For example, the Professional Seminar Series consists of pre-packaged presentations and course materials, which would be of great benefit to the IS auditing profession if they were to be presented on a regular basis, in order to target new entrants to the profession and improve the knowledge and understanding of existing practitioners. Educational courses utilizing this resource are easily arranged.

The session times at the Conference were 90 minutes, while at most Australian events 45 minutes is normal. The longer session is designed to allow a speaker time to identify a problem, discus its significance and impact or audit implications and discus solutions. This certainly works for substantial subjects. At the previous year's Australian conference session times were 30 minutes, and many attendees considered this to be neither serious nor sensible.

Project Control –
The Auditor's Role in
IS Projects/Systems Development

Tuesday 21 November 2006
10.00 to 16.30
(Registration opens at 09.30)

at

Chartered Accountants' Hall, Moorgate Place, London EC2

A one-day joint event organised by the
BCS Information Risk Management & Audit Specialist Group and
the IT Faculty of the Institute of Chartered Accountants in England & Wales

For a booking form and further information
contact IRMA administration at admin@bcs-irma.org
or visit the website at www.bcs-irma.org

IT under scrutiny

Alan Calder and Steve Watkins

IT security has a reputation as a being a barrier, rather than an aid, in the workplace. That's starting to change, and ISO 27001, the new information security standard, is already helping refocus organizational IT security activity on the actual needs of the business.

ISO 27001 is the world's first formal, internationally recognized specification for an information security management system. It has a much broader use than people might imagine but used wrongly it could become a fossil, left behind by the rapid evolution of technology and technological threats.

A new profession

Information security is a relatively new profession, but then so is the modern computer and the modern computer network. It wasn't IBM's invention of the PC, or the founding of Microsoft, but the emergence of the internet in the mid-1970s that gave birth to a new, online world in which digital data could be moved and stored in ever greater quantities and by increasing numbers of people.

Computer hackers have existed for almost as long as organizations have stored information on computers. Before the internet, hackers had to physically access a machine before they could attempt to access its data. But once the machine was permanently connected to others, the remote hacker gained opportunities galore. Then followed the virus: the first computer virus emerged only 20 years ago. And today? There are over 120,000 viruses live 'in the wild' – free on the internet.

We think of the 21st century as the information age. If this is so, then the most important component of any corporate balance sheet is its intellectual capital – the intangible assets that include:

- intellectual property, such as brands, trademarks, copyrighted and patented items
- customer and supplier databases
- individual and departmental staff know-how
- business processes
- organizational competence (the complex of know how, processes, systems and experience that enable an organization to achieve its business objectives)

Intellectual capital depends for its very existence on IT and, as we're aware, IT is vulnerable to external attack. It is also vulnerable to internal fraud in a way that, as Barings Bank learned to its cost, can destroy an organization within a matter of hours. It is also vulnerable to simple human error.

Personal privacy

It is not just corporate information which is at risk, of course. Databases containing individual and consumer personal data – names, addresses, social security numbers, credit card details – proliferate daily. They are attractive targets for identity thieves, who know they can use this information to steal millions of pounds and remove it to the other side of the world noiselessly, unobtrusively, and without danger to themselves.

Unfortunately consumers do not do much to protect themselves against these threats, either at home or in work. In a recent survey, 85 per cent of participants compromised their individual password secrecy for a Starbucks coffee – participants were offered a free coffee if they could remember (and share) their corporate password – and those who didn't want to give it away, were mostly prepared to confirm whether or not it was their mother's maiden name, or their child's birthday. Regulators have caught on: they suspect that there are votes in protecting consumers against the theft of their individual data and, as a result, data protection and personal privacy legislation is proliferating across countries belonging to the Organization for Economic Cooperation and Development (OECD).

All EU countries have implemented stringent regulations, and more than half the US state legislatures have done the same. Of course, there is no coordination between any of this legislation, so organizations operating in more than one jurisdiction (or, in some cases, having consumers from more than one jurisdiction on their database) are exposed to possibly contradictory – certainly untested – laws and regulations.

Regulatory compliance

General personal privacy is just the tip of the iceberg. There are specific sectoral requirements, like HIPAA (Health insurance portability and availability act) and GLBA (Gramm-Leach-Bliley Act) in the US, the payment card industry requirements which apply in all outlets that accept Visa and Master Card, the Financial Services Act regulations, and so on. There are also the increasingly complex audit requirements of corporate governance, which want assurance that the information and communications systems, on which the organization's accounts depend, are secure and controlled.

'IT security' – the selection and implementation of controls by the IT team – is not an effective solution to the complex range of issues the organization faces. What every organization requires is a coherent, comprehensive approach to information security that is capable of being tailored to its specific needs and circumstances. The answer is not just IT security, but information security.

In ISO 27001, information security is defined as the 'preservation of confidentiality, integrity and availability of information. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved':

- availability – 'being accessible and usable upon demand by an authorized entity'
- confidentiality – 'information is not made available or disclosed to unauthorized individuals, entities, or processes'
- integrity – 'safeguarding the accuracy and completeness of assets'

ISO 27001 systematically describes how to ensure the availability, confidentiality and integrity of information within an organization. It recognizes that threats to information arise and must therefore be addressed.

These are obviously risks that need identifying and, as with most risks, the sensible management approach is to introduce a degree of control. The challenge though is that, even if managers are able to identify all the real information security risks and the appropriate controls for them, controls cost money to implement, and it is unlikely that implementing every possible control is affordable, reasonable, or even necessary.

In the UK, organizations must also take into account the requirements of the:

- Data Protection Act
- Computer Misuse Act
- privacy regulations
- Copyright, Designs and Patents Act
- and for public sector organizations, the Freedom of Information Act

All of these have a direct impact on information management.

In 1998 a new accredited certification scheme was introduced for a standard specifying the requirements for information security management. The standards were BS 7799 parts 1 and 2 (with part 1 being a code of practice and part 2 providing the management system specification against which organizations could be assessed).

In 2000, part 1 was re-issued, with some slight amendments, as an international standard, ISO/IEC 17799. It has since been substantially revised and was re-issued in 2005, still defining a code of practice that consists largely of a list of controls to address specific risks. It has been widely adopted and its principles are reflected in standards as diverse as the payment card industry standard and US Federal Information Security Management Act.

The management system specification BS 7799 part 2, was revised in 2002, introducing the PDCA model. By 2005, the various localized versions of BS7799-2 that had been introduced around the world were replaced with a single international standard – ISO 27001 – largely based on the evolved British standard.

ISO 27001 defines the PDCA cycle as a means of introducing and implementing an information security management system (ISMS). Taking each stage of this cycle in turn, the standard requires:

- plan – define the scope of the ISMS; define the information security policy; define and conduct a systematic risk assessment – at the individual information asset level; identify and evaluate options for the treatment of these risks; select the control objectives and controls for each risk treatment decision and prepare a statement of applicability
- do – produce the risk treatment plan, including planned processes and procedures; implement the risk treatment plan and controls; provide training and awareness for staff; manage operations and resources in line with ISMS; implement procedures for diction of and response to security incidents
- check – this stage is that of monitoring, testing, audit and review
- act – the findings from the 'check' stage should be reviewed and action should be acted upon, including actions required to address changes in any factors affecting the risk

ISO 27001 and ISO 17799

Appendix A of ISO 27001 is a list of controls. There are 134 controls, contained in 12 major control areas. These controls address all the potential risk areas, from virus and mobile code through to intellectual property theft, business continuity and access control. The Annex A controls replicate those contained in ISO 17799, to which the user is directed as the source of good practice guidance for implementing the controls. In effect, ISO 27001 mandates the use of ISO 17799 while providing the management system that enables ISO 17799 controls to be part of an integrated framework.

As part of the plan phase, the organization has to prepare a statement of applicability. This, in principle, is a statement as to which of the controls listed in Annex A applies to the organization and how it is implemented. The control statement for clause 5.1 of Annex A might, for instance, be that the organization has an information security policy, which is signed off by the board, and is available to all staff and appropriate third parties on the organizational intranet. Where one of the controls is not applied, there has to be an explanation, such as the statement that controls on software development are not required as the organization sources all its software from third party suppliers.

Be business-able

While ISO 27001 provides a rigorous specification for a coherent, integrated information security management system, and one that is vendor and technology neutral, it is not a panacea. Designing and implementing an ISO 27001 system is not for the faint-hearted, and real success depends very much on three things: the risk assessment process, the real level of management commitment, and the practical, day-to-day involvement of staff and users.

It is a key principle of ISO 27001 that the only controls implemented should be those that help the business protect itself cost-effectively without undermining the business objectives. organizations that apply this principle are those in which the information security team are seen as business enablers, not business blockers. This only happens when management – from the CEO down – understand and embrace information security as a system and a philosophy inside the organization. When management provides business guidance for the security people, and helps define and implement (on an ongoing basis) the approach to risk assessment, then the organization tends to evolve a constructive approach to information security.

Evolving technology

Instant messaging, voiceover IP telephone systems, wireless networking and blogs are all technologies which are being rapidly deployed throughout the corporate world. These were originally seen as consumer technologies; they do not have the robustness of typical enterprise products or the level of inbuilt security that is now expected of enterprise products. They are, however, extremely useful, extremely easy to get into action and a nightmare for the IT security people – unless they are alert to changing technology trends and evolving threat scenarios.

In many global organizations, the information security network access policy is set by the IT team without reference to the business. As a result, the business users routinely circumvent the system by using USB sticks to move data between computers – with all the attendant risk of data loss, data corruption, and data duplication. The right response to this situation is not to deploy USB blocking technology but, all too often, that is what does happen.

These are the organizations in which information security strangles the business. Deploying an ISO 27001 system, with its emphasis on risk-based controls and management direction, might just save such an organization from itself. Inevitably though, there will be organizations that deploy ISO 27001 prescriptively, insist on implementing all the controls and ignore the principle of risk-based controls and business-orientated solutions. These organizations will not survive the changing threats that emerge from the fast-changing technology market. For instance, they will respond to users who wish to use instant messaging by disabling it, ban blogs, and make web surfing difficult.

Information security becomes more high profile every day. As corporate governance and legislative requirements develop they are increasingly including more information-related aspects. In the UK, the Turnbull guidance on internal control and risk management gives directors of public companies a clear responsibility to act on IT governance, the effective management of risk in IT projects and on computer security. It is a topic that, in the information age, is here to stay.

About the authors

Alan Calder and ***Steve Watkins*** run IT Governance Limited, a company whose website (**www.itgovernance.co.uk**) provides a comprehensive range of books, toolkits, advice and guidance to help organizations tackle IT governance and information security issues, including ISO 27001. Their book *IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799* is a plain-English guide to achieving ISO 27001 certification.

IRMA PRESENTATION

3 October 2006

16:00 for 16:30 to 18.00

at BCS, 5 Southampton Street, London WC2

LIFTING THE LID
ON STOLEN LAPTOPS!

Using a stolen laptop to access the corporate LAN
A presentation by Ken Munro of SecureTest

This meeting is FREE to IRMA members and is followed by networking and buffet.
To reserve a place email admin@bcs-irma.org or visit www.bcs-irma.org

Quick Wins For IT Management Teams

David Cuthbertson, Square Mile Systems

If you want to achieve quick wins by management initiatives, with additional long term business benefits – the best way is by process improvement. If you are also implementing management frameworks such as ITIL, BS7799, ISO20000 and CoBit then you may be able to combine project streams. Knowing where to apply focus is key – so you can improve response times and reduce capital purchases, team workloads and risk. Our white paper describes how a short infrastructure data audit can significantly shorten timescales.

What's the Problem?

Delivering IT services continues to become more difficult due to budget restrictions, improved controls, service improvement and demands to keep up with business change requirements. The various IT departments often understand their own issues, but are too busy delivering against their individual targets. It's a management problem to see across the infrastructure teams to determine what needs to be changed. If you ask the manager of any group, they can often describe why they are managing well within their boundaries, but it doesn't help when the business is more concerned about the end to end service.

IT support groups have business as well as internal IT goals and objectives – guess which takes precedence? If we also assume that IT teams have generally evolved to solve business problems using technology, it's quite a leap to expect IT staff to look inwards to define their own problems, then come up with solutions that are mainly about people and process. So how do you instigate a change programme when understanding the current processes (part of the preparation) is too difficult?

Defining The Current State.

To understand the current systems and processes across teams typically requires lots of management time and many meetings. You may use external consultants to overcome the natural disinclination to admit internal failings or problem areas. The amount of time needed to understand the start point of any project is well spent as you can avoid misunderstandings and reduce the number of assumptions. It can take a lot of effort, before there is enough detail to enable the setting of direction and objectives.

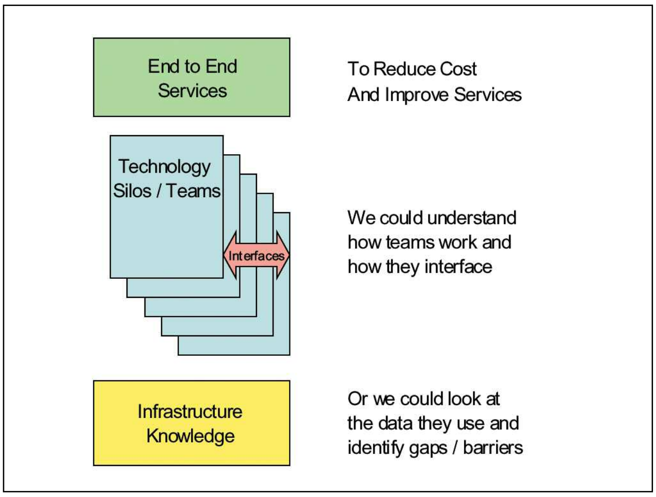

End to End Services
To Reduce Cost And Improve Services
Technology Silos / Teams
Interfaces
We could understand how teams work and how they interface
Infrastructure Knowledge
Or we could look at the data they use and identify gaps / barriers

Figure 1. – Look at the data used by the teams

Our approach is to look at the knowledge base used by teams to note commonality, gaps and duplication – taking no more than 4-5 days. If the data doesn't exist, or is inconsistent then there are opportunities for quick wins, as our case studies show. We want these quick wins to benefit the business, as well as communicating that the first steps in a management change programme have produced visible results. For any project to deliver short and long benefits through process change in IT support, understanding the current state is necessary, but not so easy.

Assessing Value and Risk for Management Led Initiatives

To make significant cost reductions, service improvements or other objectives set by the business, you have to judge the value and cost of finding information and resources for planning activities, as well as applying a good dose of risk management. The first step is to ensure there is common understanding of existing processes and gaps, rather than what is perceived or just plainly misunderstood. To define and document all the processes by which IT operates could take so long that you miss all the timescales you may have set. Every meeting can become a debating point – is this the current process or what it should be? It can get very tense if a middle manager thinks that being honest about his challenges could be misinterpreted. You may not know what to believe – so evidence needs to be collated.

Our approach of auditing the knowledge base, while not so obvious, achieves quick results to facilitate management decision making and avoid potential misunderstanding. For any organisation involved in ITIL best practice, this is often the first stage of an asset and configuration management programme. The infrastructure data audit typically highlights many issues: • Inconsistent naming conventions – preventing integration of systems

- ✔ Lack of ownership of data leading to inaccuracies or local variations
- ✔ Unnecessary duplication where too many versions of the same device exist
- ✔ Disparate sets of data held in spreadsheets, each with it's own terminology
- ✔ Network diagrams of varying age, different to the network monitoring system
- ✔ Lots of project build documents, but no "big picture", held by operations
- ✔ Individuals under extreme pressure because of past knowledge or roles
- ✔ Update processes not being followed as new policies were never defined
- ✔ Unnecessary capital spending as no knowledge of spare "stock" or capacity exists
- ✔ Outsource partners disagreeing over interpretation of responsibilities in contracts
- ✔ Departments setting own priorities in times of overload, undermining other teams Focusing on tangible items, such a server, and examining all aspects (location, power, cabling, hardware, software, systems, applications, backup, recovery, etc) reveals very quickly where the gaps in data

are, with the corresponding omissions in process. It also highlights where quick wins can be gained and incorporated within other projects. Verifying some of the data from the audit by a sample manual check makes the management team even more aware that the gaps are real.

Case Study 1 – Desktop Controls

The desktop section in a business relied on an audit package to discover all 9000 PCs on the network and the software that was loaded on them. They felt no need to develop processes, or keep an asset list as their software tool gave them “all the information they needed” about the live environment. The output of the audit software linked into the help desk system to keep it updated. In essence, they did not see the value in checking the information or conducting a manual audit as it was “probably 98% right”. We were asked to help plan a manual inventory by the operations manager, because the desktop team eventually agreed they didn’t have the resource or time to do a verification audit.

The end results – just from talking to teams during the planning exercise:

1. The desktop numbers were wrong by 15%, due to duplications within the audit package, so more software was provisioned than actually used.
2. The help desk team had stopped the automated update of their system as the duplicates caused problems when logging fault calls.
3. The audit package never deleted PCs from its audit database, plus there was no manual mechanism to dispose of PCs, to reclaim software licences, or to change the status to “disposed of” in the help desk.
4. Users had deleted or disabled the audit software on their PCs, so they had not been inventoried at all, which had caused problems with a technology refresh programme.
5. There was no knowledge of PC location or network connectivity, so all office moves still had to involve a site survey by desktop staff and often a third party contractor, who was paid every time to feed back information to planning teams.
6. The current status of PCs and their location was not known by the help desk, so it was easier to buy new PCs to meet user requests, rather than find an existing one of a suitable specification.

After a manual audit on one site, we found over 100 PCs not in use, so there was immediate saving in forecast hardware and software expenditure. After re-installation of the desktop audit agent on “lost PCs”, the desktop audit tool had the duplications and old devices removed, taking the PC population down by 10%. While the cabling and connectivity has not been documented, the costs of desktop moves are now known to be around £450 per desk. If the organisation needs to speed up office moves and reduce change costs further, it can undertake a more informed cost/benefit analysis of tackling the cabling.

If Case Study 1 sounds familiar, you can see that it requires management direction to solve these issues. The desktop, software licensing, help desk and cabling teams are all probably working hard, but not effectively. As an unexpected result, the server team heard what was happening in desktop area and documented all the servers and their cabling in the data centre – without being directed to!

What Do We Mean By An Infrastructure Data Audit – Is It a Stand Alone Project?

Square Mile prefers to use the ITIL and ISO20000 best practice frameworks as a base for our work. Much of what we do is more formally known as asset and configuration management. An infrastructure data audit is often the starting point, followed by detailed planning and data capture. We normally spend 4-5 days looking at existing operational information, analysing how it is used and kept up to date. But there is more to it.

Any piece of hardware or software used within a business goes through a typical lifecycle, as shown in Figure 2. Whether it was purchased, inherited as part of a merger, or delivered as part of a service, it came from somewhere and will eventually be disposed of. If we take a file server, the information kept by the various teams that interface with it shows us where there is common understanding, or lack of it. We know that absence of documentation is a danger sign as it prevents inter-team working, with assumptions and guess work being used to compensate. For example, if we have 50 servers on maintenance – which 50 servers? We bought 45 licences for SQL server – have we used them all? Are we using older versions? Have we recovered the licences from the servers we scrapped as part of a technology refresh?

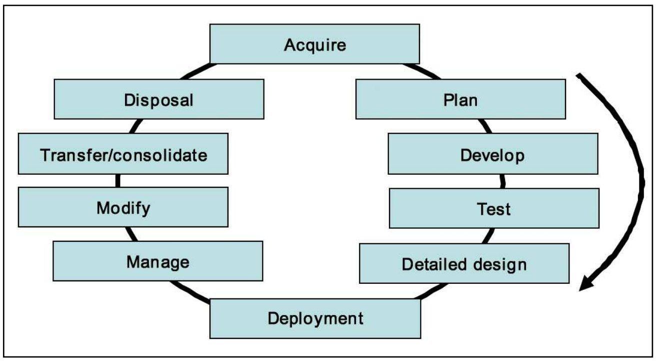


Figure 2. – A Typical Asset lifecycle

This is asset control in practice. With good controls you minimise the amount of unnecessary expenditure and confusion when dealing with internal teams and third parties. Assets can be data centres, equipment rooms, hardware, software, people, business data – it’s up to you. Basically, we should know what IT assets we have, preferably in a shared, common format.

Configuration management is a step up from asset management where we want to understand how the IT assets interact and depend on each other. It may cover how servers link to networks, or how an application relies on multiple servers and network devices, or which desktop builds have particular applications. There is considerably more detail in the ITIL framework on configuration management, though in practice it is mainly common sense and covers the various information sources we all use. As with asset management, lack of visible records is a danger sign as it shows people are relying on memory or informal communication when deciding to change a critical system, or plan an office move. More importantly, configuration management shows gaps which teams either make up for by working unnecessarily harder (think more cost), or they just ignore it as a company problem they can’t solve . If we implement even just a few configuration management practices, teams will normally work better together and processes become more streamlined.

Case Study 2 – Data Centre Optimisation

A new data centre manager was appointed to take control of the multiple data centres and equipment rooms on the major sites in a financial service organisation. A number of outages due to power or environmental problems had occurred, plus each Monday morning there was normally some disruption caused by weekend changes. As well as these tactical issues, he also had to decide whether a new data centre should be built, or to host servers externally. He found that no group "owned" the understanding of what equipment was in the data centres or rooms, so it was impossible to establish a baseline from which to manage capacity or change. He wanted to look at consolidating legacy systems using blade servers, but found that the knowledge existed only in peoples' heads so he would have to impact existing teams even to work out direction. Finally, when a power supply tripped due to a new server being installed, he realised he had to Acquire Plan Detailed design Test Develop Modify Transfer/consolidate Deployment Disposal Manage Figure 2 – A Typical Asset Lifecycle © Square Mile Systems Limited Page 4 of 4 take a lead, as it was a cross team problem. No team or individual was at fault, it was (as they say) a management problem.

An asset database was implemented containing all the hardware devices in the data centre, along with their connectivity at power and cabling level. This enforced common naming conventions, update processes and work flow across the various data centres. It also created standardisation of status, so equipment could be retired, re-used or disposed of to free up rack space, or ports on switches always had a device connected.

Consolidated reports could be run to determine the amount of free rack space and network capacity across all the data centres. Processes were developed for deployment of any equipment into the data centre so that various teams could trust the data. In hindsight, what did the manager achieve?

1. He found no need to buy additional data centre capacity for at least the next 2 years
2. He freed up 15% of rack space by disposing of unwanted kit (equivalent to half a new data centre)
3. Power phases were more evenly balanced, resulting in no disruption due to power trips
4. He saved over £300K capital purchases in the first year by re-using network switches
5. Maintenance contract costs were reduced by consolidating purchases
6. Deployment planning was reduced from multiple meetings to an email or two between project teams and data centre staff
7. Regulated systems were consolidated along recovery plans, to support faster service restoration
8. The capacity limits of the data centres were known to the IT management team so that they could assess the impact of new business requirements, or new technologies i.e. grid computing

Looking at the data used by existing teams to manage space, power, cabling, risk, recovery, etc. quickly highlighted some of the root causes of disruption that could only be solved by senior management getting involved.

In this case, asset and configuration management disciplines were applied to the data centre environments. There was an initial infrastructure data audit to help the planning and scoping of the project. This enabled the new manager to quickly determine where role changes were required and the development of a more formal deployment process to capture all new equipment entering the data centre.

Summary

Senior management need to understand where there are opportunities for quick wins, which only they can make happen. Making teams more effective and streamlining processes to reduce workload can have both short and long term business benefits, but there is a cost to getting enough of an understanding to know where to focus. In 4-5 days an infrastructure data audit quickly shows where there are existing gaps and barriers to cross team working, as well as opportunities to gain immediate business benefit.

The Author

David Cuthbertson is a founding director of Square Mile Systems, a UK computer services company based in Cirencester, England. He is an industry speaker on best practices and applying configuration management techniques to ICT infrastructure. He is also chairperson of the BCS Service Management Specialist Group (SMSG), as well as chairing the Board of Governors for the Academy of IT, a further education initiative developing vocational training for new entrants into the IT industry.

© Square Mile Systems Limited
www.squaremilesystems.com

IRMA MEETING

Tuesday 12th September 2006

16.00 for 16.30 – 18.00

at BCS – 5 Southampton Street,
London WC2

"Spreadsheet Risks: Ubiquity, Severity & Legality?"

A presentation by Grenville Croll of Spreadsheet Engineering Ltd

This meeting is FREE to IRMA members and is followed by networking and buffet.
To book a place email admin@bcs-irma.org or visit www.bcs-irma.org

HUMOUR PAGE

ACCOUNTANTS . . . and proud of it.

What's the definition of a good tax accountant?
Someone who has a loophole named after him.

When does a person decide to become an accountant?
When he realizes he doesn't have the charisma to succeed as an undertaker.

What does an accountant use for birth control?
His personality.

What's an extroverted accountant?
One who looks at your shoes while he's talking to you instead his own.

Why did the auditor cross the road?
Because he looked in the file and that's what they did last year.

There are three kinds of accountants in the world. Those who can count and those who can't.

How do you drive an accountant completely insane?
Tie him to a chair, stand in front of him and fold up a roadmap the wrong way.

What's the most wicked thing a group of young accountants can do?
Go into town and gang audit someone.

What do accountants suffer from that ordinary people don't?
Depreciation.

An accountant is having a hard time sleeping and goes to see his doctor.
"Doctor, I just can't get to sleep at night."
"Have you tried counting sheep?"
"That's the problem I make a mistake and then spend three hours trying to find it"

Comprehending Accountants Take One

Two accountancy students were walking across campus when one said," Where did you get such a great bike?"

The second accountant replied, "Well, I was walking along yesterday minding my own business when a beautiful woman rode up on this bike. She threw the bike to the ground, took off all her clothes and said, "Take what you want."

The second accountant nodded approvingly," Good choice; the clothes probably wouldn't have fit."

Comprehending Accountants Take Two

An architect, an artist and an accountant were discussing whether it was better to spend time with the wife or a mistress. The architect said he enjoyed time with his wife, building a solid foundation for an enduring relationship. The artist said he enjoyed time with his mistress, because of the passion and mystery he found there. The accountant said, "I like both." "Both?"

The accountant replied "Yeah. If you have a wife and a mistress, they will each assume you are spending time with the other woman, and you can go to the office and get some work done."

Comprehending Accountants Take Three

To the optimist, the glass is half full.

To the pessimist, the glass is half empty.

To the accountant, the glass is twice as big as it needs to be.

Comprehending Accountants Take Four

"An Accountant and His Frog" An accountant was crossing a road one day when a frog called out to him and said, "If you kiss me, I'll turn into a beautiful princess". He bent over, picked up the frog and put it in his pocket. The frog spoke up again and said, "If you kiss me and turn me back into a beautiful princess, I will stay with you for one week".

The accountant took the frog out of his pocket, smiled at it and returned it to the pocket. The frog then cried out, "If you kiss me and turn me back into a princess, I'll stay with you and do ANYTHING you want."

Again the accountant took the frog out, smiled at it and put it back into his pocket. Finally, the frog asked, "What is the matter? I've told you I'm a beautiful princess, that I'll stay with you for a week and do anything you want. Why won't you kiss me?"

The accountant said, "Look I'm an accountant. I don't have time for a girlfriend, but a talking frog, now that's cool."

Ethics in Business

"Dad, what's ethics?"

"Well, son, you know how your uncle and I are in business together? Suppose a customer comes in and buys something worth £10 but gives me a £20 note by mistake and doesn't ask for change. If I split the extra £10 with your uncle, that's ethics."

Accuracy in Business

IBM, the computer giant, decided to have some parts manufactured in Japan as a trial project. In the specifications, they stated that they would only accept three defective parts per 10,000.

When the delivery came in there was an accompanying letter. It said, "We Japanese had a hard time understanding North American business practices. But the three defective parts per 10,000 have been separately manufactured and have been included in the consignment. Hope this pleases you."

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

SIGNATURE: DATE:

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

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

Management Committee

CHAIRMAN	Ross Palmer	ross.palmer@hrplc.co.uk
SECRETARY	Siobhan Tracey	siobhantracey@aol.com
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Ross Palmer	ross.palmer@hrplc.co.uk
JOURNAL EDITOR	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 – ISACA	Ross Palmer	ross.palmer@hrplc.co.uk
MARKETING	Vacant	
ACADEMIC RELATIONS	Vacant	

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 = irmalondon
		Password = 4members06

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

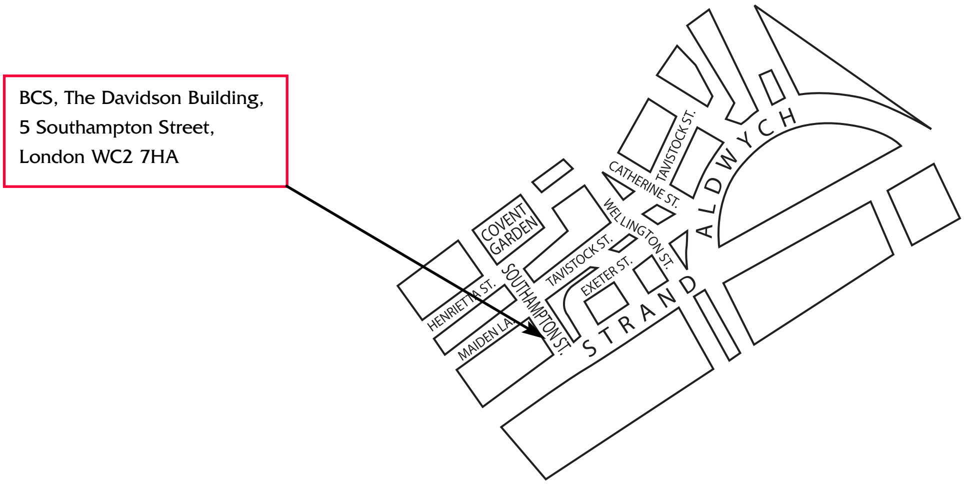
We can undertake direct e-mailing to our members on your behalf at any time outside our normal distribution timetable as a 'special mailing'. Items for distribution MUST be received at the office at least 5 WORKING DAYS before the distribution is required. Prices are based upon an access charge to our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