

President's Report

"The Titanic sank in an ocean that was 99% free of icebergs."

Mark Frautschi, Y2K microchip systems expert

Hindsight is a wonderful thing. The quote above comes from the August 1999 edition of New Internationalist. This article went on to state that *"The Y2K danger should be a wake-up call for the world and the beginning of the end of the era of nuclear terror."*

Seven years on, reading this statement only leaves me reflecting on how much and how little the world has changed. Sure, we can all be pretty smug about the Nemo-sized impact of the Y2K bug, but the terms of reference on terror and risk, where are they? How are these being played out? What are the new ground rules for risk management? Our new website, to be launched in April 2006, will have forums where such topics can be debated. Looking forward to it.

Changing of the Guard – And the Award Goes To ...

This is my last report as President of the ISACA Sydney Chapter. Yes, a bit sad. On April 19, 2006, a new Board will be elected at the Annual General Meeting of our members (further details are in this issue). It's been a two-year stint so I think I'll take this last moment to enjoy the spotlight. I'll just pop on my Oscars' style fashion earrings and say – "It's been great guys!"

Of course, I would like to thank the cast of the Sydney Chapter Board, 12 wonderful folks, who have dedicated increasing amounts of time to putting together the face of ISACA Sydney – PD Week, Technical Sessions, CISA & CISM review sessions / exams, the website, SCAN, marketing banners and not to forget the online membership survey. This is not to mention national and international boards and government forums where these folks represent our chapter and membership. As a benchmark, the amount of effort required is sometimes equivalent to a second day job, and this is very much appreciated.

This sterling effort is not only recognised by myself but also by ISACA International. We are very proud to be awarded the **K. Wayne Snipes – Best Very Large Chapter in Oceania 2005**. This is the second year running that the Sydney Chapter has received this honour. The award is given in recognition of chapter growth in membership, support for the professional development of its members and the overall direction of the group. The official presentation of all world-wide awards will occur at the *ISACA International Conference in Adelaide in July 2006*. So again great work!

I am going to take a risk and make a few special mentions.

Firstly to our Treasurer - Carmen Hawkins, who is also thankfully known as Eagle Eyes. Does anyone know how much work Treasury entails? She will tell you I'm sure.

Garry Barnes - CISM Director, who lives and breathes security, and works passionately to arrange for CISM sessions to occur and to get meaningful but challenging questions put



Mike Thompson & Garry Barnes - Sydney Chapter CISA & CISM Co-ordinators

onto exams in his role on the CISM Test Enhancement Committee. Candidates who participated in the review sessions will know that the quality of presentations/discussions is second to none and our results show it.

Mike Thompson – CISA Coordinator, worked with Garry to arrange the first running of ISACA's December exam sessions in 2005. This is no trivial feat I can assure you.

Matt Parrelli – Technical Director, this is the guy on the Board pushing to make it all happen for the website. Matt's patience and perseverance has been incredible, and that was just dealing with the Sydney Board and International counterparts on website requirements and keeping their attention for more than a few minutes.

Kurt Huth – Editor, sourcing material is hard enough, theming it up and getting it out... lots of work.

Stewart Mantell – Marketing Director, anyone who can understand International's Marketing Report requirements deserves an award. The new Banner and branding also look excellent.

(Continued on page 2)

Inside this edition	
SAP Data Access with ACL	Page 4
Job Practice Analysis Keeping - CISA & CISM Current	Page 6
The Information Security Framework	Page 7
March Technical Session Review	Page 10



(Continued from page 1)

Johan Pelser – VP, and Ken Doughty, both PD Directors, finding speakers and putting together the first PD Week were great. Our technical sessions were a sellout each time, leaving Helen juggling waiting lists.

Johannes Pricken – Membership Director, putting together our first online survey. Johannes pushed this - what a great idea and response rate!

And last but not least, my thanks to the person that makes all the magic come together and has done so for the past two decades, Helen Gulson. She makes multi-tasking look like child's play. Thanks Helen, working with 12 crazy folks and International has been a chore, but you always do it with a smile. Top stuff!

Unfortunately it has not been all trips to Las Vegas in the fall. But I have enjoyed the support of a great group of people, whose skills are matched with the dedication to make a difference. I will miss their looks of despair at 7.35 p.m. on Tuesday evenings, as we ploughed through more actions than a Geneva Convention. Good luck guys, for the impending Board elections and thanks.

Winners are Grinners – Way To Go Sydney!

In the recent CISM and CISA results released by ISACA International, of Chapters with more than 10 candidates for the December 2005 **CISM** examination, Sydney Chapter had the highest percentage of candidates passing the examination. Of Chapters with more than 10 candidates for the December 2005 **CISA** examination, Sydney Chapter is in the top ten of Chapters with the highest percentage of candidates passing the examination. What an effort!

Congratulations!



Sydney Chapter president Gladys Rouissi with Faraz Khan who top scored in the June 2005 CISA exam.

On behalf of the Sydney Chapter Board, our congratulations to Sydney's Top Scorers for the December 2005 CISA and CISM exams. These are:

CISA

- 1st place - Miriam Lane
- 2nd place - Igor Cardoso
- 3rd place - Craig Harris
- 3rd place - Brett Chaiyawat



Keith Price who top scored in the June 2005 CISM exam receiving his award.

CISM

- 1st place - Timothy Au
- 2nd place - Shaun Gollodge
- 3rd place - Chetan Trivedi

Online Membership Survey – Smashing Response Rate

Okay, we've blown the average response rate for surveys out of the water. I understand that any response rates over 4% is considered favourable. We had a 20% response rate. Great stuff and thanks to all members who responded.

Johannes Pricken – our Membership Director, is going away with all the results and will

be reporting back to the Board in April. After this I hope to see some changes that will come about as a result of your feedback.

Thank you to those that indicated special interest in being more active on the chapter, such as writing articles, assisting in arranging sessions. I know it is tough for folks to give up personal time, so we do appreciate it. One of the Board members or myself will be in contact with you regarding how we will move forward. Thanks for putting your hand up.

Gladys Rouissi

President
ISACA Sydney Chapter

ISACA Sydney Chapter

Annual General Meeting

Wednesday
19 April, 2006

at

Ernst & Young
Level 22
680 George Street
Sydney

at 5.30 p.m.

To be followed by the presentation of awards to the top CISA & CISM candidates and the April technical session

“The Challenge of IT Asset Management”

To be presented by

Ken Doughty

Darren Ramsey from Adelaide will also give us a brief rundown on the upcoming ISACA International Conference to be held in Adelaide.

(Security at Ernst & Young will require all attendees to sign in so please arrive a little earlier to give yourself time to do so.)



International Conference
30 July – 2 August 2006
Adelaide, South Australia

Activity for the preparation of the 34th International Conference in Adelaide from 30 July - 2 August 2006 is well underway. The Conference Program Committee has reviewed in excess of 120 abstracts received for the 40 available topic spots. This has ensured high quality sessions with experience speakers covering the latest topics of interest. The program is sure to obtain many sessions of interest to all IT Governance professionals across all ISACA's key lines of support.

The six pre and post conference workshops have now been set and presenters for these are being finalised as this goes to print. Again, current and popular topics for the workshops were selected from a choice of dozens. Member comments and suggested topics were considered when choosing the workshops to ensure people got what they most requested (on average).

The Adelaide sub committee members, Darren Ramsey, Howard Nicholson and Rob Hanson are also currently busy with the following:

- Seeking a Keynote speaker with a high public profile and an interesting and relevant story to tell;
- Communicating with many organisations discussing the value to them in becoming a sponsor or exhibitor at the conference;
- Organising optional chapter run social and educational events that will enhance and add to the conference value and experience.

If you work for or know any organisation who may be interested in a promotional or marketing opportunity at the Adelaide conference, contact Darren Ramsey on **Ph. 043 9977 555** or email to eitm@ramstech.com.au to arrange a further discussion.

The conference's Preliminary Brochure outlining the conference content and structure is now available and the final brochure with detailed information including session topics is within a week or so of release. Keep your eye on email and visit <http://www.isaca-adelaide.org/conferences.asp>

These brochures will assist you in discussing conference attendance with your organisation. It is shaping up to be the most prestigious event on ISACA's local calendar in many years.

Regards,
Darren Ramsey,
Conference Director,
ISACA Adelaide Chapter
Ph. +61 43 9977 555

**30 Years Strong
And Time to Party!**

Time has swissshed by and yes ISACA Sydney Chapter is turning the big 30 in 2006!

Watch this space for details of our 30th birthday celebration, which is being planned for September 2006.

If you have a special talent that can be aired in public, let me know and we can consider it for the official entertainment list.

Gladys
president@isaca.org.au



The ISACA Sydney Chapter was happy to be part of the recent Identity Management Summit held in Sydney on 7-8 March 2006, attracting over 180 attendees. There were a number of international renowned speakers who provided insight into Identity Management trends and practices.



SAP Data Access with ACL

Following the ISACA technical session "CAATs using ACL" on 28 February 2006, a number of queries have been made about the above topic. This is a common issue experienced by SAP users, as it is difficult to obtain accurate data in a timely and cost-effective manner. This article discusses the features, benefits and technical aspects of the ACL SAP DirectLink™ software solution.

Benefits / description:

DIRECT, SEAMLESS ACCESS

The SAP system is accessed directly through the ACL desktop via the menu: Data > External Data > SAP R/3.

AUTOMATIC FORMATTING

Direct Link automatically formats SAP R/3 data for use within ACL. The data does not require any manual formatting or additional data conversion. This saves time and improves productivity by eliminating the need to define and prepare data after it is extracted.

DATA INTEGRITY

Direct Link reads the data in place and cannot alter production data, thus ensuring that data integrity is always maintained.

AUTOMATION

Routine data analysis procedures can be accelerated by incorporating SAP R/3 data retrieval into existing ACL scripts. Also, if the SAP environment is standardised, the same ACL scripts can be executed on multiple SAP installations.

SYSTEM SECURITY

Direct Link and ACL feature read-only data access, which means that source data can not be modified or deleted. Access to SAP tables is determined by

the user's SAP authorisations, and the standard SAP Logon screen is accessed via the menu above.

As a result, data integrity is never compromised and SAP security is respected. Also, Direct Link uses SAP security to determine access rights, which means security setup and maintenance activities are minimised.

MULTI-TABLE QUERIES

Up to five tables can be joined prior to extraction. This allows you to bring together disparate data and drill-down for more granular data results. You can also select individual fields and apply filters to obtain only the data you need.

Data can be queried in this manner by going to Table > Add in the Direct Link interface. Tables can then be selected from a list.

FOCUSED QUERIES

Filters further streamline queries so you can extract only the records of interest. Direct Link dynamically generates ABAP programs; with self-performing syntax checks, that contain OPEN SQL statements.

FIELD-LEVEL TABLE SEARCHES

Direct Link includes a meta-data browser that allows you to search by table name and description or by SAP module. You can drill down by application area or search through tables and fields by name or description, by entering the appropriate criteria in the table search window.

FLEXIBLE QUERY EXTRACTION

Direct Link gives you the ability to run ABAP extracts.

Online extraction - for small data extracts, online extraction executes and downloads query results directly into ACL in a one-step process.

Offline extraction - for larger data extracts, offline extraction can be done during non-peak processing hours, minimising the impact to SAP system performance during high demand periods. The results are stored on the SAP server for retrieval at your convenience.

SAP TABLE TYPES

Direct Link can access all four SAP table types: Clustered, Pooled, Transparent and View.

TECHNICAL SPECIFICATIONS

SAP R/3 Version 3.1H to 4.7 (Enterprise)
One or more PCs running ACL Desktop or Network Edition (Version 7.0.2 or higher)

INSTALLATION

Direct Link requires three installations: one for the SAP system, one for the file server, and one for the workstation. A Basis Administrator and Security Administrator must install all the SAP system component. Installation times vary between two and three hours. The installation is a one-off, and then data is analysed by ACL in the usual manner.

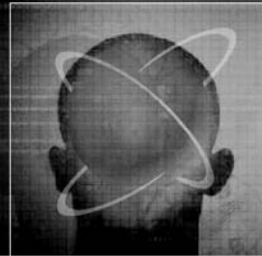
For further information, please contact Adrian Atherton on 0434 358 979, or email (aatherton@satorigroup.com.au).



**Be a better auditor.
You have the knowledge.**

We have the tools.

IDEA



Using **IDEA's** powerful functionality and robust performance, you can

- Improve your audit performance.
- Extend your capabilities.
- Lower your audit costs.

With over *40,000 new users* in the last two years, **IDEA** is clearly the leading data analysis software.

For more information about **IDEA** and to request a *Free Demo*, visit our website at www.horwathcs.com.au or e-mail us at idea@horwath.com.au.



IDEA is a registered trademark of CaseWare IDEA Inc.

Auditors in over 90 countries in 13 languages use IDEA to outperform the expectations of clients, employers and regulators.



Job Practice Analysis Keeping CISA and CISM Current

Becoming certified is an important step for any professional. While certification means many things to many people, primarily it signifies competency in your chosen career.

However, the certification choice facing audit, IT and security professions is particularly difficult. In a recent count, over 80 certifications are available to them. The certification of choice will be the one that holds its value over time, particularly in rapidly evolving fields like audit, security and IT.

This is one of the reasons candidates choose ISACA's CISA and CISM certifications. ISACA's certifications are constantly kept current to maintain validity and value.

One of the processes that ISACA employs for this purpose is "job practice analysis". In fact the 2006 CISA examination will be based on a new "job practice", as will the 2007 CISM examination.

So what is "job practice analysis"?

Job practice analysis seeks to provide a contemporary description of the role performed by Information Systems Auditors (for CISA) and Information Security Managers (for CISM). Validation of content, via job practice analysis, ensures that the certification and examination reflect current requirements for competent performance in the respective professions.

For CISA, practice analysis has taken place every five years. For CISM, even though its inaugural examination was in 2003, the first practice analysis

has now been completed in readiness for 2007.

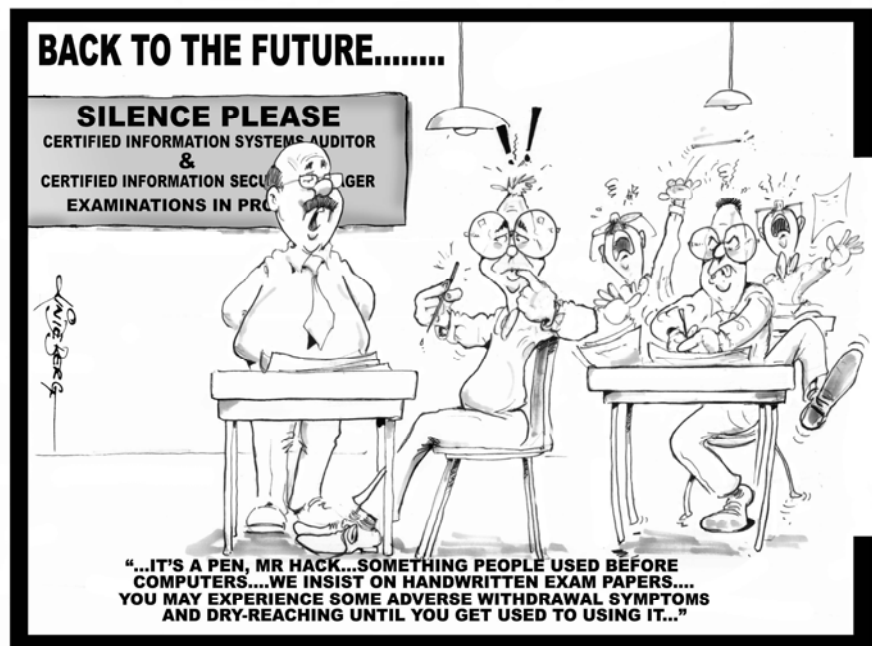
Job practice analysis involves defining and confirming the tasks being performed by CISA's and CISM's and reaffirming the required knowledge. ISACA draws upon its global reach to involve Subject Matter Experts, focus groups, email and on-line revisions and independent reviews. These processes rigorously define, refine and revalidate current job practice prior to final acceptance by the respective Certification Board.

Practice analysis is essential to ensure the validity of the CISA and CISM certifications, and to retain the high reputation of ISACA as a certifying body.

Garry Barnes
Vice President &
CISM Co-ordinator

CERTIFICATION EXAM ALERT!

- For those members who passed the CISA exam in 2001, the deadline to apply for certification is 31 December 2006. Reminders will be sent to these individuals.
- The next exam session will be 10 June 2006.
- Final registration for the CISA / CISM June 2006 examinations is 5 April 2006. Register via www.isaca.org/cisa or www.isaca.org/cism.
- Study materials for June 2006 are now available.
- You can print the CISA or CISM Bulletin of Information from www.isaca.org/cisaboi or www.isaca.org/cismboi.
- If you are sitting for the June exam and want to receive emailed results, make sure you answer 'yes' to this question (#27) on the registration form.





THE INFORMATION SECURITY FRAMEWORK

By Martin Kaldor

Information Security has rapidly evolved over the past decade. Heavily focused on the technical during the late 1990's, there is now emphasis and wide discussion on meeting business objectives.

For Information Security management, this means involvement in areas such as security governance, risk management, finance, HR, project management, CIO priorities, strategic planning, and the range of middle to upper level management concerns.

The role of Information Security Manager (ISM), while still relatively new in many organisations, is rapidly changing from perimeter security configuration and change, to providing corporate guidance, strategy and protection of information assets.

To achieve this, the IS manager needs to have or develop understanding of the organisation's business, and the contribution to be made by information security.

This needs comprehension of how information security can contribute to both the achievement of business objectives and risk management. It means the management ability to explain information security issues in 'business-speak', the sales capability to 'sell' information security to CIO and organisation business process owners, and the recognition of where (and how) to contribute ideas and solutions from the IS resources to other areas such as communications, IT and HR.

It also requires awareness of all the documents contributing to information security

development - legal/regulatory (such as Sarbannes-Oxley, Privacy Act, Workplace Surveillance, etc.) plus information security standards (ISO 17799/27001 and any of the other 100+ ISO standards, AS/NZS documents) plus industry guidelines (COBIT, ITIL, SANS, COSO, HB231, CERT, Homeland Security) and valuable vendor guides (eg CA, Cisco, Microsoft). (Does this qualify the ISM for a salary increase?)

So with the ISM contributing as a middle to senior level enterprise manager, the ISM needs to have the enterprise focused vision of how information security comes together to contribute to the organisation.

The ISM needs a methodology to bring together all the areas of concern - anti-spam/anti-virus with corporate governance, Sarbannes-Oxley compliance with 'Unified Threat Management', management reporting with acceptable use policy, and many, many more.

The ISM today is overloaded with information, with many valuable sources of 'How to Develop and Manage Information Security'. From these, the ISM needs to build a framework to meet all requirements, and then tailor this to the organisation activities.

With all the resources previously outlined, information overload is very possible. Indeed, there is a danger of the ISM spending so much time amalgamating all the guidance, standards, and 'how to' information, and being occupied in communicating with the organisation regarding risks and requirements, that

implementing security gets forgotten.

Hence the obvious - the ISM needs a framework to structure the various information security issues and activities.

Creation of a Framework creates the vision of the ISM, as to what needs to be considered from an overall perspective, and the areas/activities that are needed to build the organisation's Information Security environment for its business requirements.

This framework should not provide a detailed, itemised information security checklist. This would be too extensive. It must cover the top levels of overall areas of potential activity and the main activities within each area. The main activity areas will typically involve different personnel in different groupings (i.e., Security governance will not involve the same people as network security).

There are many systems that can be used as the starting point for developing a framework. However, the rapidly growing enthusiasm for CISM, and the knowledge base on which CISM is based, provides a good starting point.

CISM covers five management areas:

- Information security governance
- Risk management
- Information security program management
- Information security management, and
- Response Management

(Continued on page 8)



Membership Renewals

2006 membership dues are now overdue. If you have not renewed your 2006 membership, now is the time to do it! You can do this online at www.isaca.org - click on the link to My ISACA.

For those people also paying their CISA and/or CISM, please ensure you fill in your CPE hours.

Thank you to all members who completed our online membership survey. We have had a tremendous response with 20% of members making the effort to complete the survey. Once the information has been collated and evaluated all members will be advised of the results. The Board will be able to utilise this information in its forward planning.

*Johannes Pricken
Membership Director*

(Continued from page 7)

This provides a good start for a framework, but from my perspective provides straight-line progression and hence needs to close the loop by providing management feedback, such as compliance assessment and management reporting.

The reporting now needed is not the basics of how many viruses or port scans were stopped, but should relate back to the management requirements outlined in governance, i.e., progress on support of business objectives.

So if we consider starting from the Executive Management/ Board level requirements, and looping back to provide feedback, then the Framework starts to look like **Diagram 1** below.

From the Australian perspective, CISM does not include ISO 17799, an increasingly major part of the required framework.

The 17799 structure contributes to the Information Security Program Development/Security Management area. This can

also cover the Response Management area from CISM.

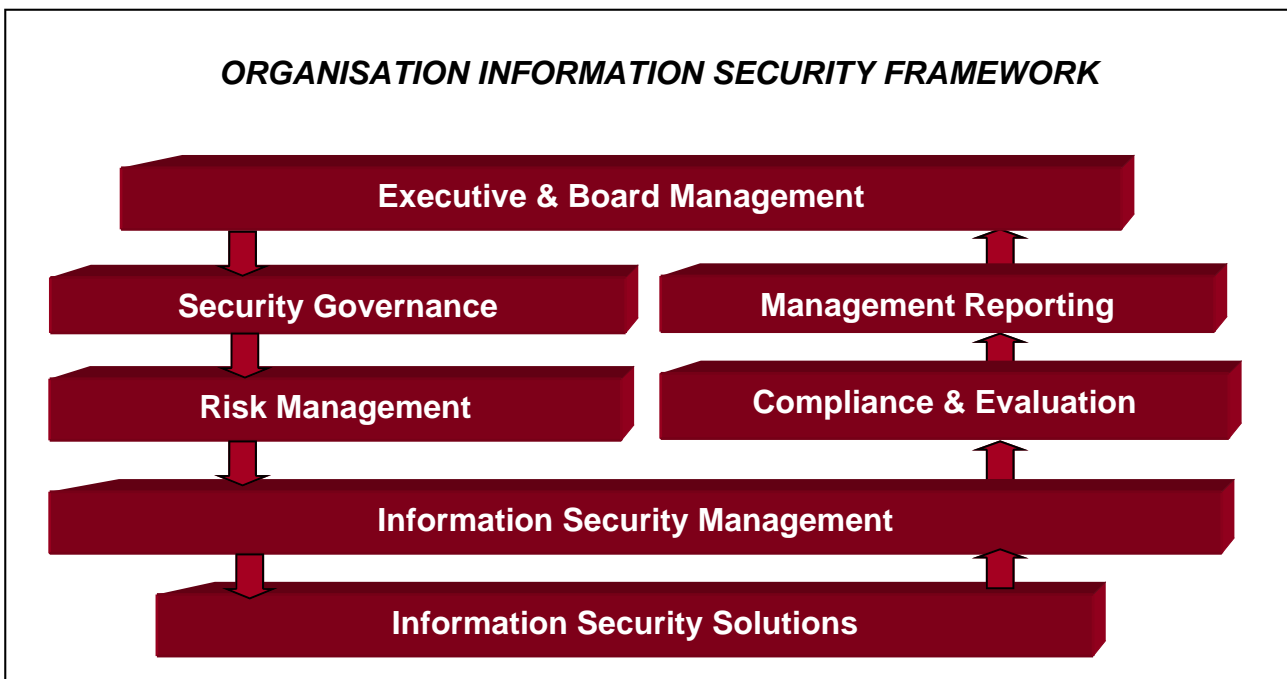
So if we expand the Framework areas to include the issues identified, then our overall Framework becomes as seen in **Diagram 2** on page 9 opposite.

With such a Framework, the ISM is equipped to undertake development of specific activities, one at a time, randomly, in each of the areas, while still maintaining an overall vision of how the total Information security environment comes together.

Martin Kaldor BE MBA (CISM exam completed) is a Director of Shearwater Solutions, long serving Excom member and past Chair of AISA, and a member of the Sydney Chapter of ISACA.

(Continued on page 9)

Diagram 1





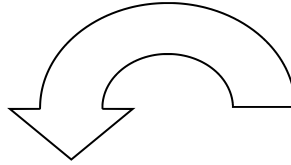
(Continued from page 8)

Diagram 2

EXECUTIVE & BOARD MANAGEMENT

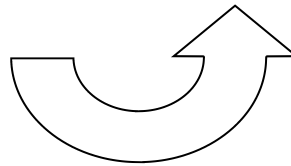
GOVERNANCE FRAMEWORK
IS Strategy
Management Commitment
Roles and Responsibilities
Communication Channels
Legal and Regulatory
IS Policies
Procedures and Guidelines
Value Analysis

MANAGEMENT REPORTING
Governance Objective Reporting
Risk Management & Risk Change Reporting
Information Security Reporting
Event Reporting



RISK MANAGEMENT
Risk management process
Life cycle integration
Risk identification analysis methods
Risk mitigation
Reporting risk changes

COMPLIANCE & EVALUATION
17799 Legal Compliance
17799 Policy Reviews & Technical Compliance
17799 System Audit
Awareness Training Compliance



INFORMATION SECURITY PROGRAM DEVELOPMENT	INFORMATION SECURITY MANAGEMENT	ISO 17799	RESPONSE MANAGEMENT
		Create & maintain plans	Rules of use compliance
Information security baseline(s)	Administration compliance	Organisational Security	Develop response & recovery plans
Business process procedures/guidelines	Outsourced service compliance	Asset Classification and Control	Test response & recovery plans
IT infrastructure activity compliance	Measure, monitor, reporting metrics	Personnel Security	Response & recovery plan execution
Life cycle activities	Change management process	Physical & Environmental Security	Event documentation procedures
End user impact	Vulnerability assessments	Communications & Operations Security	Post-event reviews
Owner accountability	Non-compliance issue resolution	Access Control	
Establish Metrics	Culture & behaviour development	Systems Development and Maintenance	
Internal & external resources		Business Continuity Management	



WHAT IF YOU'RE CALLED IN AS AN EXPERT WITNESS?

As an expert witnesses, you must maintain your independence and avoid altering your reports to suit the needs of litigants.

In *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (the "Kazaa Case"), the trial judge discredited the bulk of the expert evidence given by Professor Ross, a respected Computer Scientist. In cross examination Professor Ross admitted that his expert report was based on an initial "skeleton report" provided to him by the defendant's instructing solicitors, and that he agreed to their changes to the technical aspects of his report.

The court concluded that Professor Ross was seriously prepared to compromise his independence and intellectual integrity. After this evidence, the court found it might be unsafe to rely upon Professor Ross in relation to any controversial matter.

If you are called upon to act as an expert witness, your duties include:

1. An overriding duty to assist the court impartially on matters relevant to the expert's area of expertise.
2. A paramount duty to the court and not to the person retaining the expert. Accordingly, an expert witness is not an advocate for the party.
3. Your duty to follow the Federal Court Guidelines for Expert Witnesses or other appropriate guidelines in fulfilling your duty.

Although it is appropriate for you to collaborate with lawyers on the form of your report, it is not acceptable for litigants or their lawyers to influence its content. The Kazaa Case highlights the need for care to be taken in communications between an you, a litigant, and its lawyers. Generally, such communications are protected from disclosure until the your report is served on the other party.

The NSW Government may be considering the introduction of punitive sanctions against expert witnesses found to have behaved dishonestly or unprofessionally.

Dr Stephen James (NSW Bar)
Associate Director
NSW Internal Audit Bureau

March Technical Session Review

On 15 March Garry Barnes presented an interesting and informative technical session on 'Developing a Successful Information Awareness, Training and Education Program'.

Garry began by highlighting the fact the word 'successful' had been included in the title of his presentation specifically to make the point that there were a number of factors which needed to be taken into account when designing a security awareness program to ensure that it was effective.

Garry asked "what is the weakest link? Is it technology, processes or people?" The answer: "people are the weakest link". According to the 2004 AusCert Computer Crime and Security Survey "changing user attitudes and behaviour regarding security practices" was the most challenging security management problem

for organisations.

A key message was that everyone in the organisation should receive basic security awareness training. The four points a security awareness program should get across to the end user about security are:

- What is it?
- Why is it important?
- What is required of me?
- Where do I go for help?

Garry explained that further education and training may be required according to peoples' roles and responsibilities, relative to information assets. For example, system administrators with higher privileged access may require training above and beyond that given to a standard employee.

Garry described the steps in raising user awareness levels. These include considering the basic goals you want the awareness training to achieve; understanding the organisational culture in order to determine the

focus; target your message - that is "who are the key groups and/or roles you wish to get your message across to?"

You should also keep in mind the following critical success factors before putting your security awareness, training and education program into action:

- Need for executive support
- Program encompasses everyone
- Message is aligned
- Delivery methods are varied
- Must be a continuous process

Garry outlined multiple methods of delivery available. These include bulletins, brochures, posters, videos, quizzes (with perhaps a prize attached), lunch time sessions or executive one-on-ones. Those which provide some sort of incentive are much more likely to get people involved and the message across.

Craig Jones



Light up your potential in Hong Kong & China *

Make a move to PricewaterhouseCoopers and we will not just broaden your mind. With a client base that is the envy of the region, plus a complex and challenging workload, we can also add some breadth to your CV.

PricewaterhouseCoopers (www.pwc.com) is one of the world's largest professional service organisations, which provides industry-focused assurance, tax and advisory services for leading global, national and local companies and public institutions. Our worldwide network comprises of over 130,000 people in 148 countries, with approximately 260 partners and 6,500 staff in Hong Kong, Macau and mainland China.

SYSTEMS & PROCESS ASSURANCE – HONG KONG, BEIJING, SHANGHAI & GUANGZHOU

Working with our leading clients in key industries in the Systems & Process Assurance team, you will gain exposure to a wide variety of complex operational and systems environments, challenges and learning opportunities. Assignments will include performing risk assessments, technical and general computer control reviews, business process/application controls reviews, IT security reviews, and other controls and assurance related work, both for Sarbanes-Oxley related projects and supporting our financial audit teams. For people with stronger IT or process consulting backgrounds, there will be opportunities to get involved in a variety of non-audit advisory, technology and performance improvement assignments.

Senior Associate / Manager / Senior Manager

Requirements:

- University degree majoring in accounting, information systems and computer science
- Professional qualifications: CPA, Certified Internal Auditor or CISA
- Minimum of 2 years system or controls assurance experience with a reputable international accounting firm or multi-national corporations
- Practical experience in two or more of the following – business & system processes review, IT auditing, IT risk management and internal audits
- Hands-on exposure to Sarbanes-Oxley requirements is desirable
- Excellent communication skills in both oral and written English and Chinese (including Mandarin)
- Effective project management, interpersonal and influencing skills are essential
- Flexibility to travel to out-of-town engagements
- 5+ years of working experience required for Manager position

Application:

Interested applicants, please send detailed resume, quoting “SPA-SA/M/SM(SYD)” and stating your preferred location(s), to assurance.hr.hk@hk.pwc.com.

Applicants not being invited for an interview within 10 weeks may consider their applications unsuccessful. Applicants who have applied in the past 12 months are not required to submit their application again. Personal data provided by job applicants will be used strictly in accordance with the Personal Data (Privacy) Ordinance a copy of which is available on request and will be provided immediately on receipt of your request.

©2006 PricewaterhouseCoopers. All rights reserved. PricewaterhouseCoopers refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. *connectedthinking is a trademark of PricewaterhouseCoopers.



Information Systems Audit & Control Association
PO Box 254 Northbridge NSW 1650
Telephone: (02)9958-0143
Fax: (02)9967-4191
Email: helen.gulson@isaca.org.au
www.isaca.org.au

Journal Update

The Information Systems Control Journal is seeking articles for Volume 5, 2006 to be issued in September 2006. The copy deadline is 24 May 2006 and the theme is **Shifting Governance Roles & Responsibilities**. For more information email jblader@isaca.org.

Advertising Prices (includes GST)

	SCAN Only	Web Only	SCAN & Web
Full Page	\$660.000	\$275/month	\$715/issue & month
Half Page	\$330.00	\$275/month	\$550/issue & month
Quarter Page	\$165.00	\$275/month	\$400/issue & page

If you would like to place an advertisement in SCAN or on our website, or for any enquiries, please contact Helen Gulson on (02)9958-60143 or email her on helen.gulson@isaca.org.au.

Conference Update

7-11 May 2006 - North America CACS, Orlando, Florida, USA

30 July-2 August 2006 - International Conference, Adelaide, South Australia

For full details about these conferences, check out www.isaca.org/conferences

2005/2006 ISACA Sydney Chapter Board

President	Gladys Rouissi	9312-7698	president@isaca.org.au
Vice President & PD	Johan Pelser	9261-1090	vice_president@isaca.org.au
Vice President & CISM	Garry Barnes	9244-0149	cism@isaca.org.au
Secretary	Andrew Bissett	9691-9505	secretary@isaca.org.au
Treasurer & IPP	Carmen Hawkins	0418-761-009	treasurer@isaca.org.au
Membership	Johannes Pricken	8233-8170	membership@isaca.org.au
Editor	Kurt Huth	8232-7746	editor@isaca.org.au
PD Director	Ken Doughty	0419-487-301	education@isaca.org.au
Marketing Director	Stewart Mantell	9226-1340	marketing@isaca.org.au
Technical Director	Matthew Parrelli	9322-5209	technical@isaca.org.au
CISA	Mike Thompson	8253-1590	cisa@isaca.org.au
Director	Richard Stapleton	9372-0841	director@isaca.org.au
Administration Manager	Helen Gulson	9958-0143	helen.gulson@isaca.org.au