

LOGON

THE NEWSLETTER OF THE CANBERRA CHAPTER INC
INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

MESSAGE FROM THE PRESIDENT

In October, I attended the Oceania President’s council meeting which was held in conjunction with the OceaniaCACS. President council meetings occur twice a year to discuss matters of mutual concern in relation to the operations of the Association in the region. Areas discussed include:

- OceaniaCACSs conferences. Future location of CACS conference. These are Sydney in 22-26 September 2003, Melbourne in October 2004 and Perth in 2005. A working group as been established to examine options for changing structure of the conference and to determine whether there are any ways to improve sponsorship and marketing. I am a member of that working group.
- International conference. There is general agreement that there is value in having an International Conference in this region at some time. Prior negotiations have fallen through. Adelaide is proposing to put forward a proposal for 2006.
- Common approach to promoting IT governance. A paper on a common approach that I prepared was discussed and it was agreed there was a broad agreement about a common approach to promoting IT governance within the region.
- Privacy Statement. A draft privacy statement was provided by Perth.

The Canberra board met to consider directions for the chapter in 2003. The meeting was very productive. More detail on this will be available at the Annual General meeting.

The success of the chapter is a result of the hard work put in by the members of the board. Two of our longer term members, Andy Edwards (Treasurer) and Kristine Johnson (Secretary, membership and web pages) have indicated that they don’t intend to

continue on the board next year. I would like to express my thanks for their considerable efforts. They will be missed.

If there is anyone willing to assist the chapter either on the board, in a sub-committee or even to assist once off in the running of workshops or technical sessions please contact me by email at shanahan@ozemail.com.au or on 0417 802 544.

Max Shanahan
 President

IN THIS ISSUE	
NOTICE OF ANNUAL GENERAL MEETING.....	2
TECHNICAL SESSIONS	2
COURSES.....	2
CHAPTER PRESIDENT WINS AWARD.....	2
OCEANIA CACS 2002.....	2
CHAPTER FEES 2003.....	3
CISA NEWS.....	4
INFORMATION ABOUT CISM.....	4
WEBSITE UPDATE.....	5
JOURNAL UPDATE.....	5
CANBERRA CHAPTER BOARD.....	5



*Information Systems
 Audit and Control
 Association*

Notice of Annual General Meeting

of the Canberra Chapter of ISACA

5.30 pm Tuesday 3 December
Canberra Club, West Row, Civic

Two lucky members who attend will win door prizes of wine or a book voucher (to the value of \$50)

Agenda and Notice of Meeting will be distributed early November.

TECHNICAL SESSIONS

Congratulations to Roger Kaufmann who won a free registration at CACS 2002 just by attending a technical session during the year. The Board are offering the same prize to one lucky member who attends a technical session between now and August 2003. Make sure you RSVP and sign the registration sheet at each session to be in the running.

There has been a great range of tech sessions in 2002 with topics ranging from Cyberforensics to Website Security Vulnerabilities and Knowledge Management. The September technical session was presented by Dr John Mitchell, a keynote speaker from the CACS 2002 conference, who shared his experiences in auditing an E-commerce environment. The session was enjoyed by around fifty members and associates, most of whom took time out afterwards to catch up with colleagues and friends over drinks.

2002 has also seen ISACA present a series of joint sessions with the Institute of Internal Audit. The last joint session for 2002 will be at the Canberra Club on 22 October with the topic "Better Practices in Report Writing".

The final session for 2002 will be "The SAP Audit Information System" on 19 November, before we break for Christmas and bounce back in 2003 with a February session on "Auditing a Public Key Infrastructure".

The board are determining a programme of topics for 2003 in the next few months - if you want to see a particular topic presented, or would like to present something yourself, please contact Patrick Kevin ♦

COURSES

The very successful Fundamentals of IS Audit course was run again in August. In fact demand was such that the course was run twice. We will be running this course again in 2003. We are also considering running an Advanced IS Audit course.

Due to resource constraints, the SANS Institute Windows 2000 Security course has not yet been run but is being considered.

Further information on any of these courses can be obtained from Lorraine Stevens ♦

MAX SHANAHAN WINS THE JOHN LAINHART AWARD

When he attended the Global Leadership Conference in New York in July, Max Shanahan, Chapter President was presented with the John Lainhart award. This award is to recognise individuals for contributions to the development and enhancement of the Common Body of Knowledge used by the constituencies of the association in the field of IS audit, security, and/or control, IS audit certification, and/or IS audit standards. It is intended to be used only when individuals far exceed the norm, and is granted by two-thirds approval of the Association Board. Congratulations Max!

OCEANIA CACS 2002

Well, as the advertising says, the weather was pretty close to perfect. And the company was good, the presentations were interesting, even if the conference dinner was not quite as good as the one Canberra put on last year (in my humble unbiased opinion). There was no dancing!

Many of the speakers referred to the various moves worldwide to strengthen corporate governance. They referred to the recommendations of the Turnbull Report in the UK and the Sarbanes-Oxley Act (2002) passed in the US.

- The Turnbull Report describes guidelines to help directors of listed companies set up sound internal control systems to managed significant risks. Listing rules now require that a company must explain in its annual report and accounts the extent to which it has complied with the guidelines. (More information on the Turnbull report and its implementation is available at the site of the Institute of Chartered Accountants in England and Wales, www.icaew.co.uk)

CONT...

cont...

- The Sarbanes-Oxley Act (2002) includes a variety of provisions; independent audit committees, disclosure of off-balance sheet provisions, protection for whistleblowers, executive bonuses to be forfeit if accounts need to be restated, and the penalty of up to **20 years** imprisonment for anyone who *"..knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States.."*

(The Sarbanes-Oxley Act can be found via the US Senate website at www.senate.gov and the site of the US Securities Exchange Commission, www.sec.gov gives information about rules developed to implement the provisions)

Several speakers also spoke about the increasing use of ISO 17799 (Information Technology - Code of Practice for Information Security Management) in the UK and Europe and the fact that similar measures are being considered in the US. The OECD have also recently released guidelines, OECD Guidelines for the Security of Information Systems and Networks (available from the OECD site at www1.oecd.org)

Local speakers talked about developments in Australia. This included Division 12 of the Commonwealth Criminal Code (1995) which deals with corporate criminal responsibility and which attributes fault to a corporation if corporate culture exists which encourages or tolerates an offence, or if the corporation fails to create and maintain a corporate culture which requires compliance. Mention was also made of the Commonwealth government's decision, earlier this year to allocate \$24.9 m to the Critical Infrastructure Protection Group whose focus is on the protection of the Telecommunications, Finance, Electricity and Transport infrastructure.

There were also some good sessions on more technical issues. Some that I particularly enjoyed were the presentations on Security Metrics for Internet Gateways, Using the SAP Audit Information System, Electronic Commerce Audit in the Demilitarised Zone and Effective Penetration Testing Techniques for IS Auditors.

A few bit and pieces of trivia along the way:

- When Stanley Rifkin stole \$US 10m by means of illegal funds transfer from a bank, and was then caught as he came back into the US with the

diamonds he had bought with the money, the bank he took the money from made a \$3m profit on the diamonds.

- Bacon takes 10 weeks to cure.
- During the Gulf War, hackers broke into US Defence sites and stole information on their military plans on behalf of an international information broker who then tried to sell the information to Iraq - but Iraq didn't trust the source of the information and didn't buy it.
- The CIA detects an average of 250,000 unsuccessful hacking attempts on their site each year.
- In 2001 a Forrester Report found many Fortune 500 companies spent more on coffee than they did on IT Security.

There was also a brief presentation by the Sydney Chapter on CACS 2003. It will be held at the ANA Harbour Hotel from 22 - 24 September 2003. It looks like they have some pretty interesting overseas speakers lined up including Charles Gates from the USA who has won the Presidential Award for his work in cybercrime and in tracking pornography rings, and Frank Yam from Hong Kong who is an internationally acclaimed speaker on IT Security issues. Should be interesting♦

Kris Johnson

THANK YOU FROM THE CHAPTER -

THE BOARD AND MEMBERS OF THE ISACA CANBERRA CHAPTER WISH TO OFFER THEIR THANKS TO ACUMEN ALLIANCE AND TO ERNST & YOUNG FOR THEIR CONTINUING SUPPORT OF THE CHAPTER THROUGH 2002.

CHAPTER FEES IN 2003

Due to the relatively healthy financial position of the Chapter at present, the Board has decided that once again, the chapter component of the annual member subscription will be \$0 for 2003♦

Another new word: Blamestorming

(Sitting around in a group discussing why a deadline was missed or a project failed, and who was responsible.)

CISA NEWS

The chapter has been advised that 10 people sat for the CISA examination in 2002 in Canberra and all 10 of those candidates passed the exam. Congratulations to Phil Hargraves, Daryl Pereira, Bruce Legge and Jane Holzapfel. The chapter Board would like to acknowledge at the Annual General Meeting all those who passed the exam but we are not advised of all the names. So please, if you passed the exam this year, let someone on the Board know about it.

This may be an appropriate time to remind members who are CISAs of the Continuing Professional Education (CPE) requirements. The CISA continuing professional education policy requires the attainment of continuing professional education hours over an annual and three-year certification period. CISAs must comply with the following requirements to retain certification:

- Attain and report an annual minimum of twenty (20) continuing professional education hours.
- Submit annual continuing professional education maintenance fees to ISACA international headquarters in full.
- Attain and report a minimum of one hundred and twenty (120) continuing professional education hours for a three-year reporting period.
- Respond and submit required documentation of continuing professional education activities if selected for the annual audit.
- Comply with ISACA Code of Professional Ethics.

The annual reporting period begins on 1 January of each year. The three-year certification period varies and is indicated on each annual invoice and on the letter confirming annual compliance.

For newly certified CISAs, the annual and three-year certification period begins on 1 January of the year succeeding certification. Reporting continuing professional education hours attained during the year of certification is not required. However, hours attained between the date of certification and 31 December of that year can be used and reported as hours earned in the initial reporting period.

A CISA must obtain and maintain documentation supporting reported continuing professional education activities. Documentation must be retained for a minimum of eighteen months following the end of each annual reporting period. Documentation should be in the form of a letter, certificate of completion, payment receipt, attendance roster, Verification of Attendance form or other independent attestation of completion. At a minimum, each record should include the name of the attendee, name of the sponsoring organization, activity title, activity description, presenter name(s), activity date and location, and the number of continuing professional education hours awarded or claimed.

Activities that qualify for continuing professional education include technical and managerial training. This training must be directly applicable to the assessment of information systems or the improvement of audit, control, security or managerial skills to ensure a proper balance of professional development is attained. Continuing professional education hours are not accepted for on-the-job activities unless they fall into a specific qualifying professional education activity. Specific activities have annual continuing professional education hour limits.

The following categories of qualifying activities and limits have been approved by the Board and are acceptable for continuing professional education;

- ISACA and non-ISACA education activities, eg conferences, seminars, workshops etc
- Self study courses
- Vendor sales and marketing presentations (10 hour limit)
- Teaching, lecturing, presenting
- Publications
- Exam question development
- Passing related professional examinations
- Serving on ISACA Boards and Committees (10 hour limit)
- Contributions to the IS Audit and Control profession (10 hour limit)

A random sample of CISAs is selected each year for audit. Those CISAs chosen must provide written evidence of previously reported activities that meet the criteria described in the Qualifying Professional Education Activities. The Board will determine the acceptance of hours for specific professional educational activities.

Be aware that it is also possible to apply for Retired CISA or Non-Practicing CISA status. See the ISACA International website for details.
(www.isaca.org)

Information about the 2003 CISA examination and new, Revised CISA review materials are available at the ISACA bookstore ♦

MORE INFORMATION ABOUT CISM

More information about the new CISM certification has been released, particularly regarding the **grandfathering provisions** which may be of interest to some members.

CISM, the Certified Information Security Manager is ISACA's next generation credential and is specifically geared toward experienced information security managers and those who have information security management responsibilities. CISM is designed to

cont...

cont...

provide executive management with assurance that those earning the designation have the required knowledge and ability to provide effective security management and consulting. It is business-oriented and focuses on information risk management while addressing management, design and technical security issues at a conceptual level. While its central focus is security management, all those in the IS profession with security experience will certainly find value in CISM.

From now **until 31 December 2003**, experienced information security managers and those who have information security management responsibilities can apply for certification as a Certified Information Security Manager™ (CISM) without taking the CISM examination. To earn the CISM designation during this period, information security professionals are required to:

1. Submit verified evidence of eight (8) years work experience in the field of information security. Five (5) of the eight (8) years of work experience must be gained performing the role of an information security manager. In addition, this work experience must be broad and gained in four of the five "job practice analysis" domains. (For further information, visit www.isaca.org/cism.)
2. Adhere to the Information Systems Audit and Control Association's *Code of Professional Ethics* and agree to comply with a continuing education policy.
3. Pay an application fee of US \$495 for ISACA members or US \$595 for non-ISACA members.

Substitutions for work performed in the role of an information security manager are not allowed. However, substitutions for general work experience in the field of information security may be obtained as follows:

- A maximum of two years of work experience may be substituted for currently holding one or more of the following:
 - Certified Information Systems Auditor™ (CISA®) in good standing
 - Certified Information Systems Security Professional (CISSP) in good standing
 - Graduate university degree in information security
- A maximum of one year of work experience may be substituted for one of the following:
 - One full year of information systems management experience
 - Currently holding a skill-based security certification (e.g., GIAC, MCSE, CBCP, CompTIA Security +)

For further information on the the grandfathering provision refer to ISACA's web site which also has a downloadable application at www.isaca.org/cism "

WEBSITE UPDATE

We're looking for feedback from members on the revamp of your chapter web site (www.isaca-canberra.org.au) to make it as useful as possible to all our members. We're looking for answers to the following questions:

- what would you like to see that isn't available now?
- what business would you like to transact with ISACA through the web; and
- what web resources do you currently have bookmarked and use in your work?

The site is there for your benefit - so speak up and make your needs known! Contact Patrick Kevin or Steven Doyle ♦

JOURNAL UPDATE

The *Information Systems Control Journal* is seeking articles for volume 1, 2003, to be issued in January 2003. The copy deadline is 31 October 2002, and the theme is **Advanced Audit Techniques and Technologies**. Specifically, the *Journal* is searching for articles on topics such as continuous auditing, biometrics and wireless technology. Please view the 2003 editorial calendar, www.isaca.org/jrnl_cal.htm or e-mail jblader@isaca.org.

CANBERRA CHAPTER BOARD:

PRESIDENT	MAX SHANAHAN
VICE-PRESIDENT	STEVE DOYLE
SECRETARY	KRIS JOHNSON
TREASURER	ANDY EDWARDS
CISA CO-ORDINATOR	LORRAINE STEVENS
TECH SESSION CO-ORDINATOR	PATRICK KEVIN
DIRECTOR	SIAN RAMSDEN
DIRECTOR	SCOTT MACKENZIE
WEBMASTER	KRIS JOHNSON

CORRECTION:

In the July issue of this newsletter we incorrectly stated that new Board member, Scott MacKenzie was employed by Ernst & Young. In fact Scott is employed by the Royal College of Nursing, Australia ♦