



President's Report

Greetings to you all from London!

Congratulations – CISA & CISM Candidates

First up, congratulations to all candidates who passed the CISA and CISM examinations in June 2005. Excellent results came through, in particular for CISM exam sitters. Sydney CISM candidates achieved a pass rate of 91%, compared to a world wide pass rate of 71%. Sydney's CISA sitters achieved a 70% pass rate versus the world wide average of 52%. Well done to all.

Special congratulations must go to Sydney Chapter's top CISA & CISM scorers:

CISA:

- 1st Faraz Khan
- 2nd Jamaría Kong
- Aeq 3rd Irene Chong, Rowan Clarke, John Greaves & David Schubert

CISM:

- 1st Keith Price
- Aeq 2nd James Lassetter & Daniella Traino
- Aeq 3rd Stephen Bird & Graham Ellis

There will be a presentation to these successful candidates later in the year.

CISA/CISM Receive ANSI Accreditation

ISACA has just confirmed that the American National Standards Institute (ANSI) has awarded accreditation under ISO/IEC 17024 to ISACA's Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) certification programs.

Accreditation by ANSI signifies that ISACA's procedures meet ANSI's essential requirements for openness, balance, consensus and due process. With this accreditation, ISACA International anticipates that significant opportunities for CISAs and CISM's will continue to open in the US, and we believe it will be a strong motivator for similar recognition by governmental entities outside the US.

ISACA notes that ANSI's accreditation:

- § Promotes the unique qualifications and expertise our certifications provide
- § Protects the integrity of our certifications and provides legal defensibility
- § Enhances consumer and public confidence in the certifications and the people who hold them
- § Facilitates the mobility of certified individuals across borders or industries.

Security Alliance

ISACA has entered into an alliance with ASIS International (ASIS) and the Information Systems Security Association

(ISSA). This alliance brings together more than 80,000 global security professionals with a broad base of security backgrounds and skills to address these issues.

Locally discussions are taking place between ISACA Oceania Presidents and key representatives from these organisations to understand what benefits can be attained for our collective members. We will bring further details to you as we progress.

Support for Hurricane Katrina Victims

ISACA sends heartfelt sympathy and support to victims of the Hurricane Katrina tragedy. Our prayers go to those affected by this disaster and in particular to hundreds of ISACA members in the New Orleans area. ISACA has made a donation to the American Red Cross, an organisation that immediately mobilises workers to aid disaster victims.

CACS 2005 - Perth

Registrations are still open for the Annual Oceania CACS conference to be held in Perth from 24-26 October, 2005 and we hope to see lots of Sydney Chapter members attending.

The next International Conference – Adelaide 2006

Adelaide is the destination for ISACA's next International Conference. The conference takes place between 28 July and 3 August 2006 at the Adelaide Convention Centre. Holding this event will require considerable effort on the part of our Adelaide counterparts. Our support, in attending the conference, is critical to their success. Pencil it into your training plans for next year. Further information will be

(Continued on page 2)

Inside this edition	
Greater Scrutiny of IT Controls under Sarbanes-Oxley	Page 2
Professional Development	Page 6
CISA & CISM Report	Page 9
Workplace Surveillance Bill 2005	Page 10



(Continued from page 1)

President's Report (continued)

sent on to you as it becomes available.

Is our job as auditors important?

We talk about the boom in the assurance industry and the proliferation of standards, resulting from the Enrons and HIHs of the world. We all play our respective parts in providing assurance to the world that the risk of these recurring will be minimised. This work is critical. No doubt.

But never has the importance of our role as auditors seemed so clear as today. My current trip to New York and London has been an eye opener to the professional and emotional impact that recent tragic events have forced on us.

There are new expectations from our clients. There is less room for complacency regarding business continuity / disaster recovery. These are now taken very seriously.

Tragically 56 lives were lost in close proximity to our London office in July this year. Seeing the Hurricane Katrina disaster and being in New York on September 11 this year, made me realise again that the improbable can be real.

Our role protects the human element. It is not just saving data and assets. Getting it right, keeping up knowledge on best practice in disaster recovery, evacuation procedures, business continuity is critical. Getting it right may one day make a considerable difference.

Gladys Rouissi

President
ISACA Sydney Chapter

Greater Scrutiny of IT Controls under Sarbanes-Oxley

Peter Tighe

The Sarbanes-Oxley Act (SOX) of 2002 is a legislative response by the United States Congress to address vulnerabilities in financial reporting in the wake of huge corporate collapses such as Enron and Worldcom.

The Act, which applies to US and foreign companies that report to the United States Security and Exchanges Commission (SEC), must include in their quarterly filings an attestation by CEO and CFO on the company's internal control over financial reporting. Under s302 of the Act, the CEO and the CFO are required to assert:

- That they are responsible for establishing and maintaining internal controls;
- Have so designed internal controls to ensure that material information is made known;
- That they have evaluated the effectiveness of internal controls (within 90 days prior to the report); and
- Based on that evaluation have presented in their report their conclusions about the effectiveness of internal controls.

Core to the enforcement of the Act is s404, which requires that the external auditor provide an independent report on controls as part of its annual audit. Specifically, this requires the auditor to provide an independent assessment of how management arrived at its conclusion in its quarterly assertions under s302 filings.

The Act came into force for US companies in 2004. Evidence based on US experience indicates auditors are playing hardball on SOX s404 certification. In April, the SEC held a roundtable session to

solicit opinion on the impact and effect of SOX compliance. Based on a survey of submissions, one could conclude that the business community was generally supportive of the legislation, but the requirements demanded of companies by their auditor to comply with s404 were excessive, unreasonable and lacking judgement. Companies have complained that complying with the Act is not only a significant financial burden but has created an environment where they risked becoming uncompetitive and were considering delisting as an alternative to ongoing SOX compliance.

Furthermore, in some instances, CEOs and CFOs were finding themselves in the situation where s302 filings were being contradicted by the auditors' s404 reports - a situation most CEOs and CFOs understandably are not comfortable with. The auditors at this stage don't appear to be blinking. At a recent US symposium to discuss SOX, a senior partner from one of the big four firms was quoted in response to various criticisms by CEOs and CFOs in attendance "...that's the law so you all better get used to it".

The IT managers of Australian companies affected have until mid next year to get their house in order for SOX s404 certification in order to comply.

IT controls within organisations are of course regularly audited. This may appear to ameliorate concerns about the need to do anything differently. However, under SOX, IT controls take on a sharper focus, as the IT manager is now required to demonstrate to the audit committee and board that the organisation has effective IT controls in place. This includes



the requirement that IT controls are tested on an ongoing basis to ensure their effectiveness.

Identifying, assessing, documenting and testing IT controls are at the core of any IT SOX initiative. Till now, this is something that most IT organisations are only superficially aware of let alone proficient at. This article explores some of the challenges that IT managers face in becoming SOX compliant. The journey begins with a painstaking review of processes and procedures to understand what controls are in place and, once identified, what to do about it.

In attempting to develop an appropriate IT Control framework, many organisations are opting to use COBIT. COBIT has been around for over ten years and is recognised as the bellwether for control practices for IT. Its recent run of popularity, however, is directly attributed to SOX. The reason being that, despite its own merits (or otherwise), it is the universal standard adopted by all four audit companies to assess IT controls.

The architects and contributors to the COBIT framework have linked the COBIT processes and control objectives to the control requirements specified under the rules of the Act, namely the COSO framework. Consequently, organisations that demonstrate compliance with the COBIT framework for IT controls can, with reasonable assurance, pass the SOX s404 audit.

A note of caution for IT organisations attempting to implement a control framework using COBIT- this activity is a fundamental organisational change program. From an organisational perspective it should be seen on the same scale as an ISO or similar type undertaking. The most common failing is to underestimate the management commitment,

resources, time and effort required.

Setting out realistic objectives for the SOX compliance is fundamental to retaining focus and commitment throughout the lifecycle of any SOX project. Trying to fix everything in the first year is probably not the best way to proceed. Such an approach dilutes management focus. As in Aesop's Fable, The Man, the Boy and the Donkey, the lesson "attempt to please all, and you will please none" should be adopted as a mantra.

Under s302 and s404 companies are required to disclose any material gaps in their control gaps in their control framework. While there is a natural tendency for CEOs and CFOs to want to report a clean bill of health, this may not be the most appropriate response. Indeed, in order to satisfy their SOX obligations, companies are realising that reporting gaps is okay. The regulator is not launching investigation based on control gaps being reported, however the regulator's attention is being drawn to instances when s302 filings and the s404 appear to contradict, or when the auditor advises the SEC of a material gap.

In the context of s404 audit the author suggests, the IT organisation is focused on those areas that are currently drawing the most fire from both the regulator and auditors. The real culprits from an SOX perspective for the IT organisation are segregation of duties and change control. Consequently, the author suggests that IT organisations begin their SOX compliance effort by ensuring there are robust controls in these areas, and these are tested on an ongoing basis to satisfy s302 requirements.

Although most IT organisations are able to demonstrate some degree of control exists in these areas, it often does not extend to the level of maturity and

robustness that auditors believe is necessary for s404 signoff.

The challenge most IT organisations face is understanding and documenting what they currently do and identifying what controls exist within their processes. Although some IT processes will be documented, it's unlikely controls will have been documented to the extent that they satisfy the s404 audit.

Where relatively comprehensive process documentation exists, then the controls may be documented with reference to existing process documentation, otherwise it will be necessary to begin by documenting process from scratch. This activity is generally not a welcome proposition for IT personnel, who generally see their role as more important to that of a process analyst, and who would rather be making the change.

Management is also likely to regard this as poor utilisation of its valued IT resources. The alternative is to hire process analysts to undertake this task. There are multiple reasons not to outsource this activity, not the least being that a pile of documentation is provided at the end of the activity which internal people either don't agree on, don't understand, complain about the quality of and won't signoff on.

The next step and challenge is reconciling what IT processes should be achieving, as per the COBIT control practices against what they are currently doing. In assessing the extent to which the current processes and controls meet SOX s404 audit requirements, guidance is available from the COBIT framework. When identifying, developing or documenting controls the following needs to be considered:

(Continued on page 4)



(Continued from page 3)

- The purpose of the control (what is it designed to prevent or detect);
- Who is accountable/responsible for the control (name the role);
- Who performs the control (name the role); when, where and how often the control activity is performed;
- What format is the evidence of the control and where is it recorded/stored;
- Does the control verify other controls, (describes the relative importance);
- What COBIT control objective is satisfied.

In the company's quarterly filing to the SEC, s302 requires that controls are evaluated for ongoing effectiveness, and any material gaps be disclosed. In this context it is important to consider the effectiveness of the IT controls we have identified and documented, and how these controls will be evaluated to meet the s302 requirements.

Typically, processes contain a large number of controls. Fortunately, organisations are not required to attest to the effectiveness of all controls, but rather as specified in the Public Company Accounting Oversight Board (PCAOB) guidelines, organisations must attest to key controls. The importance of this distinction is that the number of controls documented will contribute exponentially to the effort required to manage, test and maintain documentation for on an ongoing basis.

What is a key control and how is it identified? When identifying what is a key control, the following needs to be considered. A key control is often a go/no go point in a process. A key control verifies that all other controls in the process have been satisfactorily completed.

Finally, we should review the controls documented within a

process, and ask:

- Have all controls been identified and are they sensible?
- Are the controls at sensible points in the process (eg, not too late)?
- Have the target key COBIT Control objectives been satisfied?
- Have other key COBIT Control objectives been satisfied?
- Is there inadvertent reliance or dependence on other controls?
- Can the control be tested?

Now that we have documented our processes and controls, the next step is verifying the processes are adhered to and that our controls perform as expected.

Understanding how effective our controls are is verified by a walkthrough of the process and gathering actual evidence that the control activity has been performed and appropriate action taken. To illustrate, a key control in the change control process is that changes are appropriately authorised. Under the COBIT framework, authorisation should be provided by the system owner, which is normally the business unit manager, as well as IT management. If the organisation does not already have an effective IT governance regime in place, then before an organisation can proceed to satisfy this particular COBIT requirement, it needs to begin by addressing basic IT governance requirements.

In many IT organisations, the business owner may only be consulted on functional changes. IT often implements technical changes without business signoff. Although this is not prohibited, the circumstances and rules need to be clearly understood. The auditor in their assessment of IT controls will require supporting documentation to substantiate

management decisions for what constitutes appropriate controls, particularly if in their opinion such exceptions could reduce the effectiveness of the controls.

For each key control identified, the organisation must test and record the results of such testing to support the SOX s302 attestations. It is important that IT management and stakeholders understand that what works from a simple process perspective will not necessarily work from an ongoing control s302, s404 testing perspective.

While the rewards of this effort may be debatable, the good news is that once these core control requirements are satisfied then many other dependent processes and controls from a COBIT standpoint are also satisfied. A better managed and better controlled IT is an ongoing challenge, IT organisations can use their SOX requirements to help deliver this outcome.

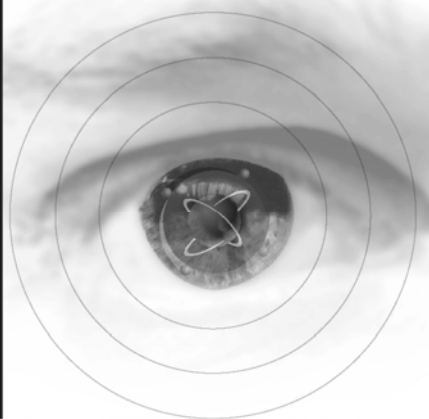
References: COBIT (www.isaca.org), COSO (www.coso.org)

Peter Tighe is a highly experienced IT consultant specialising in IT assurance, risk management and IT governance. He has held senior consulting and management positions including IT Practice leader for KPMG Middle East and director PricewaterhouseCoopers' Global Risk Management Solutions Group in Sydney.

Peter's experience encompasses: developing and assessing IT strategies, assessing IT organisation performance, including establishing appropriate governance policies, procedures, accountabilities and performance metrics. He is currently assisting a large financial organisation with its SOX compliance efforts. He holds a masters degree in IT law and masters in operations research from the University of Technology and a BSc from University of NSW.

Re-printed from Voice&Data June 2005 edition, with permission of the publisher www.VoiceandData.com.au

See it right the first time.



Unhappy with your current audit software?

Still using a spreadsheet for your data analysis?

Take this opportunity to look at

IDEA 2004

IDEA™ is recognized as the global standard against which other data analysis tools are measured. **IDEA** is used extensively throughout Australia in Federal, State and Local Government, Accounting Firms, Banking and Financial Services, Manufacturing and Retail, and in Universities as a teaching tool.

With **IDEA**, you can read, display, analyze, manipulate, sample or extract from data files from almost any source. **IDEA** provides a unique combination of powerful functionality and ease of use.

IDEA 2004 adds these key new features:

- Full text search across multiple fields and files
- Support and functions for time data types
- Action fields to allow drill across multiple files
- A new sampling module – classical variables sampling
- XML Import
- Enhanced functionality for the equation editor
- Enhanced Print file importing
- Enhanced Field statistics and charting

...all functions and tasks benefit from ease of use enhancements.



Contact us for more information – idea@horwath.com.au
www.horwathcs.com.au

Visit our stand at CACS 2005 to receive your free demo.

IDEA is a registered trademark of CaseWare International Inc.



PROFESSIONAL DEVELOPMENT REPORT

As always, we have a number of PD activities planned for our members and we are seeing excellent member turnout, especially for the technical sessions. The August and September technical sessions saw a focus on computer forensics and we lead into this quarter's PD report with some technical session summaries prepared by two of our members.

August Technical Session

And then there was business forensic computing

Over the last few years, there has been an increased interest in the field of forensics, and it primarily owes its popularity to the likes of CSI and its off-shoots which have added a glamorous sheen to it. As per the television shows, we normally relate this to the medical arena. However, it can be applied to all areas where processes and activities can be further isolated and analysed into individual components.

Jo Stewart-Rattray from Vectra Information Security presented an insightful session on 17 August 2005 to introduce business computing forensics. She defined forensics as "the collection, preservation, analysis and in some cases, the court presentation of computer related evidence which has either been generated by a computer or has been stored on computer media". In her presentation, she provided some eye-opening though unsurprising facts underlying the reason why computing forensics has come into its own as a field of study. This is mainly due to the world-wide increase of computing activity, both at work as well as at home. And of course, there is the usage of computers as a tool to commit crime.

Although the term connotes the technical aspect, forensics comprises four equally important elements:

- Obtaining the evidence
- Isolating the evidence (i.e., prevent contamination)
- Analysis of evidence (i.e., reach a conclusion)

- Possible presentation of the evidence in court.

A key point to take away from the presentation was the importance of ensuring the pristine quality of digital evidence. Although it merely adds another dimension to the universe of auditing, this is best done by an expert. It means that the question: "Is it possible that the evidence may be presented in court?", should be identified at the outset of investigation. It means that where the answer is yes, personnel with expertise in preserving and protecting the validity of the evidence should be involved as early as possible.

Reviewed by:

Amit Srivastava
Westpac Banking Corporation

September Technical Session

Computer Forensics

If you miss the monthly ISACA tech sessions, you are denying yourself a chance to extend and expand your understanding of Information Technology Universe. September's session was an excellent example of just how broad and how deep this universe is.

Nigel Carson's presentation style is relaxed and confident, and his expertise, computer forensics, is a fascinating and complex field that is relevant to all IS/IT Auditors.

Nigel comes to ISACA with an excellent track record in information technology forensics

and computer crime detection and analysis. With a degree in Information Technology from Sydney University, Nigel started his journey into forensics with the Police Computer Crime Unit and has worked with KPMG, Price Waterhouse Coopers, Roads & Traffic Authority, and Coke Cola. Nigel is currently the Director Forensics IT at Ferrier Hodgson. Nigel commented that his time at RTA and Coke as Information Security Manager added another dimension to his forensic practice expertise.

Nigel stressed throughout the presentation the interactions of IT Forensics with the legal system, and particularly the constant challenging of computer forensics in the court system. Computer forensics is a relatively new "science" and establishing acceptance at law of the tools and techniques and the evidence collected is still achieved on a case by case basis.

Computer forensics essentially started in response to the common and regular use of microcomputer for business. The original forensic tools were extremely basic, consisting principally of a safe DOS boot disk and a text editor, and relied heavily on the experience and knowledge of the analyst to read and reconstruct text fragments directly from the hard disk.

Forensic tools have evolved in line with the evolution of PC networks, and the current suite of software is both more intuitive and more easily available, although the software cost may still be significant. Nigel suggested that a computer forensics unit may need a range of PC hardware, operating systems, software and transfer & storage devices to successfully address different forensic projects. There is no single "silver bullet" that will cover the entire universe. Information that once was held on a 5 Megabyte disk on a stand alone computer can now reside on Multi-Terabyte local, LAN, WAN and ISP/ASP



disk storage, in emails, on removable drives, optical storage and an infinite variety of other media. Also this information is not limited to raw data but may include metadata, routing information and DRP sources.

Nigel offered his views on the skill set an analyst should have to undertake forensic work. These included:

- o An enthusiasm and affinity with IT (diverse experience with hardware, operating systems, software and data)
- o An investigative mindset (note taking, evidence gathering and chain of custody)
- o A capacity to represent as an expert witness in court proceedings (overt and helpful presence with the ability to withstand hostile challenges to data, evidence, tools and techniques)
- o A practical understanding of forensic tools and the underlying technology protocols (and an ability to revert to first principles if necessary)
- o Qualifications in IT and experience in the industry.

Nigel briefly discussed the “new” concepts of eDiscovery, which is becoming the twin partner of IT forensics. With more than 80% of information created and stored electronically (and a majority of this never printed), the legal sector has gone through a paradigm shift in the discovery of evidence for court proceedings. Where a single final document used to exist for legal challenge, now there can be a many variants of a document, from first rough draft to final product, and including comments asides and other essentially internal business sensitive information.

Nigel made the point that eDiscovery is the “Aerial photographic” to the Forensics “Microscopic View” of a project. And the vast quantity of data found by eDiscovery can in fact

defocus an issue. The legal community is now attempting to limit eDiscovery to expedite matters.

Nigel briefly led us through the forensic brief he prepared for the court case against Kazaa and MP3Free. This case study was both topical and relevant to our audit community.

It became obvious that evidence must be collected and collated across the range of locations and host computers and derived data becomes just as significant as the discovery fact. Nigel commented that not all sites you visit display a cooperative environment and some are exceedingly hostile, and so the need to be relatively self sufficient (computers, storage media, cables and even monitors may need to be in the tool kit you take to recover data). The fact that all defendants were found guilty of breach of copyright law is vindication of the diligence and probity of Nigel’s methodologies and practice.

Nigel presentation is on the ISACA Sydney website and his contact details are:

Nigel Carson,
Director, Forensic IT
Ferrier Hodgson
Level 17, 2 Market Street
SYDNEY NSW 2000
Phone: 02 9286 9999
E-mail: ncarson@syd.fh.com.au

Thanks again Nigel.

=====

ENDNOTE

Once again Helen Gulson did the same excellent job enlisting Nigel Carson, arranging the venue, booking the room to “sell out” capacity and organising the lunch.

=====

Reviewed by:

**Stephen Singleton, CISA
Senior IT Auditor (IT Security & eCommerce)
Roads & Traffic Authority NSW**

Upcoming PD Events

Technical Sessions:

19 October - Security Risks with Blackberry Devices
Presenter: Ian Hughes, GISG

16 November - TBA
14 December - TBA

Workshops:

4 November - Auditing Business Continuity - one day workshop
Presenter: Ken Doughty

2 December - IT Auditing and Control Self Assessment - a half day workshop
Presenter: John O’Driscoll, CBA

From the editor

Some time ago we floated the idea of moving to an “electronic version” of our SCAN newsletter. After some initial research and inquiry of our members we deferred the move having concerns around the newsletter being lost in the inundation of SPAM as well as a need to upgrade our website. The idea has not been permanently shelved and will continue to be assessed as part of the ongoing enhancement of our Sydney Chapter website. Members’ views on this matter are sought.

This will be my last issue as SCAN editor. A changed role within my organisation will see my energies spread more widely necessitating a scale back in my ISACA activities. My thanks and best wishes go to my fellow directors on the Sydney Chapter Board.

I would also encourage members to use SCAN as a means to voice their views, exchange ideas, and “get published” – its great to see your name attributed to an article published for your peers (and there’s a little monetary kicker for articles that do get published not to mention valuable CPE hours). If you wish to contribute content to SCAN please email Helen at helen.gulson@isaca.org.au.

**Kurt Huth
Editor**

New ISACA Logo

At its recent June meeting, the ISACA Board of Directors adopted a new image for ISACA. The new image consists of two elements:

- Use of the acronym only, not the full name of the association
- A new tagline: Serving IT Governance Professionals

Here is how it looks:



The purpose of this message is to give you some background information on how the change came about, why the board felt a change was necessary, what will happen next and how it will impact you.

Background

The idea of using a tagline was first broached more than a year ago, when it was recognised that ISACA's full name did not acknowledge the current composition of the membership or ISACA's increasing emphasis on serving the growing need for good IT governance within organisations. ISACA's members, CISAs and CISM's play a key role in establishing effective IT governance within an enterprise and constitute an integral part of its success.

Two options were considered to address the situation: (1) a name change, or (2) use of the acronym with an explanatory tagline.

Because ISACA has achieved a significant level of recognition over the years under its current name, there was no desire to undergo a name change. Instead, option 2 was identified as an efficient and effective way to convey the association's broadened area of expertise, while still maintaining ISACA's well-known identity.

(A tagline for ITGI—Leading the IT Governance Community— was also created to help convey the institute's purpose and role. The ITGI logo will not change; it will simply include the tagline.)

To begin the tagline selection process, an in-depth messaging session involving volunteer leaders and staff was conducted by Ketchum PR firm. By identifying and capturing the two organizations' key messages, it became possible to narrow down the types of concepts that needed to be expressed in a tagline.

In May, two taglines were selected for testing. The taglines created were designed to be similar, to underscore the close relationship between the two organizations, yet different, to emphasize their distinct purposes and target audiences. Emphasis was placed on IT governance as the overarching discipline that incorporates the many professional niches filled by ISACA's and ITGI's constituencies: IT audit, assurance, control, security and governance.

To ensure that the taglines selected reflect members' and external parties' understanding of the organizations' purposes and objectives, they were submitted to ISACA chapter presidents, longtime association leaders, IT and business reporters and industry analysts for review and comment. Although both taglines received high approval ratings from

the internal and external respondents, the chapter leaders had a few suggestions for improving the proposed ISACA tagline. The final tagline adopted addresses their suggestions to the greatest degree possible.

What Happens Now

The switch to the new association image will become effective 1 January 2006. Between now and then, a variety of activities will take place at the international level:

- A logo is being designed for each chapter, including a translated (if necessary) version of the tagline. These logos, along with a graphics standards manual showing how to use the logos, will be provided to chapters by the end of the year.
- In addition, chapters will be offered up to US \$500 to help defray their costs in reprinting chapter materials. Additional funds will be available as well, to be granted based on submission of an appropriate business case.
- All printed materials (excluding books) will be revised. This includes not only brochures, but also regular work documents such as forms, membership cards, invoices, business cards and check stock.
- The ISACA and ITGI web sites will be revised.
- Redesign of the *Journal*, *GComm* and *ExpressLine* mastheads will be investigated.

We anticipate a very smooth and uneventful transition to the new image. If you have any questions about how the change will affect chapter activities, please do not hesitate to contact any of your chapter officers.



December 2005 CISA & CISM Program

Congratulations to all those members who passed the June CISA & CISM exams. The Chapter achieved a pass rate of 70% in the CISA and 91% in the CISM - much higher than the worldwide average. The Chapter will be holding an awards night later in the year to acknowledge the top scorers. In addition, we will be issuing CISA & CISM pins to those members who have become certified in the past 2 years.

The CISA & CISM exams will be held again this year on 10 December. This is the first time these exams have been held twice in the one year. To date over 75 people have registered in Sydney for the December CISA exam and over 30 people have registered for the CISM exam. Sydney Chapter is again running a series of Review Sessions for both the CISA and CISM to help candidates prepare for the exam. Whilst the Review Sessions have already commenced, it is not too late for people to attend the remaining sessions.

The **CISA Review Sessions** commence on Tuesday, 11 October, 2005 and will consist of eight 2 hour sessions held in the evening once a week for eight weeks. These sessions will be held at KPMG Auditorium, Ground Floor, 10 Shelley Street, Sydney.

The **CISM Review Sessions** commence on Thursday, 6 October, 2005 and will consist of eight 2 hour sessions also held in the evening once a week for eight weeks. The sessions will be held at Frame Group, Level 11, 189 Kent Street, Sydney.

These sessions are open to exam candidates and general members alike. As well as assisting candidates prepare for the examinations, it is a good opportunity particularly for registered CISAs and CISM's to brush up their knowledge on the various aspects of the CISA & CISM programs.

Registration

If you are interested in registering for the review sessions or have any queries, contact Helen Gulson on 9958-0143 or helen.gulson@isaca.org.au. The cost for the whole series is \$55 for members and \$150 for non-members. Good luck to all those sitting the December exams!

MIKE THOMPSON – CISA Co-ordinator
Phone: 8253-1590
Email: mikethompson@westpac.com.au

GARRY BARNES - CISM Co-ordinator
Phone: 9244-0149
Email: garry.j.barnes@det.nsw.edu.au

CISA REVIEW SESSION DATES

11 October (Tue)	The IS Audit Process (Li Feng Wu)
18 October (Tue)	Management, Planning, and Organisation of IS (Lambros Lambropoulos)
26 October (Wed)	Technical Infrastructure and Operational Practices (tba)
1 November (Tue)	Protection of Information Assets (tba)
9 November (Wed)	Disaster Recovery and Business Continuity (Ken Doughty)
15 November (Tue)	Business Application System Development, Acquisition, Implementation and Maintenance (Naresh Iyer)
28 November (Mon)	Business Process Evaluation and Risk Management (tba)
TBA December	Examination Preparation (Garry Barnes)

CISM REVIEW SESSION DATES

6 October (Thurs)	IS Governance (Garry Barnes)
12 October (Wed)	Risk Management (John Greaves)
19 October (Wed)	Information Security Program Management (Part 1) (Martin Kaldor)
26 October (Wed)	Information Security Program Management (Part 2) (Martin Kaldor)
2 November (Wed)	Information Security Management (Part 1) (Stephen Frede)
9 November (Wed)	Information Security Management (Part 2) (Stephen Frede)
16 November (Wed)	Response Management (Rob McMillan)
TBA December	Examination Preparation (Garry Barnes)



WORKPLACE SURVEILLANCE BILL 2005

A topical area as this legislation took effect 7 October 2005

The Bill replaces and expands the current *Workplace Video Surveillance Act 1998* in a number of respects. Current provisions governing overt and covert video surveillance remain largely the same, but are expanded to cover computer and tracking surveillance within the workplace. The new Bill limits an employer's ability to block or monitor employees' emails or restrict access to the Internet unless the employer acts in accordance with an Email & Internet Access Policy which has been notified to employees. The Bill also introduces some new restrictions on the use and disclosure of surveillance records. Failure to comply with its requirements is a criminal offence, for which a director of a company may be personally liable.

Computer surveillance

- Computer surveillance means monitoring or recording an employee's use of a computer, including sending and receiving emails and accessing Internet websites.
- Computer surveillance is allowed where the employer has notified employees of the fact and nature of the surveillance at least 14 days in advance of commencing the surveillance. Notification may either by a written notice (which is clearly visible on or in the vicinity of the computer), or by audible announcement or pop-up screen notice when the employee logs-on and starts a program that is the subject of the surveillance.
- Any other computer surveillance is deemed to be covert surveillance for which the employer must seek authorisation of a covert surveillance authority on the grounds that they suspect the employee is involved in unlawful activity at work.

Blocking of emails/Internet access

- An employer may continue to block delivery of emails or access to certain websites provided it is acting in accordance with an applied Email & Internet Access Policy which has been notified to

employees and (if preventing delivery of an email) the employee is immediately notified (by email or otherwise) that the email has not been delivered. This notification is not required for emails which constitute spam, which would result in harassment or which are objectively offensive.

- Employers must ensure that they have a written notice about, or a pop-up link to, the Email & Internet Access Policy when the employee logs on to the computer or logs on to the Internet or email system.
- The Email & Internet Access Policy cannot provide for blocking of emails or Internet access simply because they contain information on industrial matters.

Implications for employers and auditors

- Organisations should conduct an audit of current workplace surveillance practices and identify any procedures that may need to be implemented in light of the new legislation.
- As authorisation for covert surveillance can only be given in limited circumstances, employers should try to ensure that as much surveillance as possible is overt.
- Employers who wish to block emails or Internet access should check they have an appropriate Email & Internet Access Policy in place and ensure that this is notified to employees. They will also need to devise an IT solution to provide a written notice about or a pop-up link to the Email & Internet Access Policy when the employee logs on or starts the relevant program.

**Dr Stephen James (ABA)
Associate Director
NSW Internal Audit Bureau**

Note: *This paper does not constitute legal or other advice and is provided for informational purposes only.*

Note also, tracking and computer surveillance are also permitted if the employee has agreed to the use of the surveillance for a purpose other than surveillance of employees (such as for security reasons) and the surveillance is carried out in accordance with that agreement. This agreement can be negotiated through a Union or other collective representative.

2006 CISA & CISM Study Materials

2006 will see some changes to the CISA job practice areas. Below you will find details of the study materials which will be required for both the 2006 CISA & CISM exams.

CISA Study Materials

The 2006 Certified Information Systems Auditor™ (CISA®) study materials are based on the new 2006 CISA job practice analysis and have been significantly enhanced with current IS audit practitioner issues.

The study materials include: *CISA Review Manual 2006; CISA Questions, Answers & Explanations Manual 2006; CISA Questions, Answers & Explanations Manual 2006 Supplement*; and the CISA Questions, Answers & Explanations CD-ROM 2006.

The new CISA job practice analysis areas include:

- The IS Audit Process
- IT Governance
- Systems & Infrastructure Life Cycle Management
- IT Delivery and Support
- Protection of Information Assets
- Business Continuity and Disaster Recovery

CISM Study Materials

The 2006 CISM study materials are based on the tasks performed by information security managers and the knowledge necessary to manage, design and oversee an enterprise's information security program. The CISM job practice areas are:

- Information Security Governance
- Risk Management
- Information Security Programme Management
- Information Security Management
- Response Management

The study materials include: *CISM Review Manual 2006; CISM Questions, Answers & Explanations Manual 2006; and CISM Questions, Answers & Explanations Manual 2006 Supplement.*

All these publications are available at:

www.isaca.org/bookstore



Sydney Chapter Website Update

The new Sydney Chapter website is nearing completion with final implementation changes being made. The enhancements include a complete re-design using multimedia of the current website with a new knowledge management section that will allow our members to collaborate online and gain access to professional information. A search engine will be added so that members can find information they require and a photo gallery to show our periodic events.

We expect this to be live for use within the next month and to aid in maintaining the forums, we are asking our member community to assist by choosing to be moderators for various areas based on their experience to the profession. Therefore, if you would like to participate and help out the Sydney Chapter, please send an email through to technical@isaca.org.au.

Matthew Parrelli
Technical Director



Oceania CACS

23-26 October 2005

Burswood Casino, Perth

“Striking a Balance”

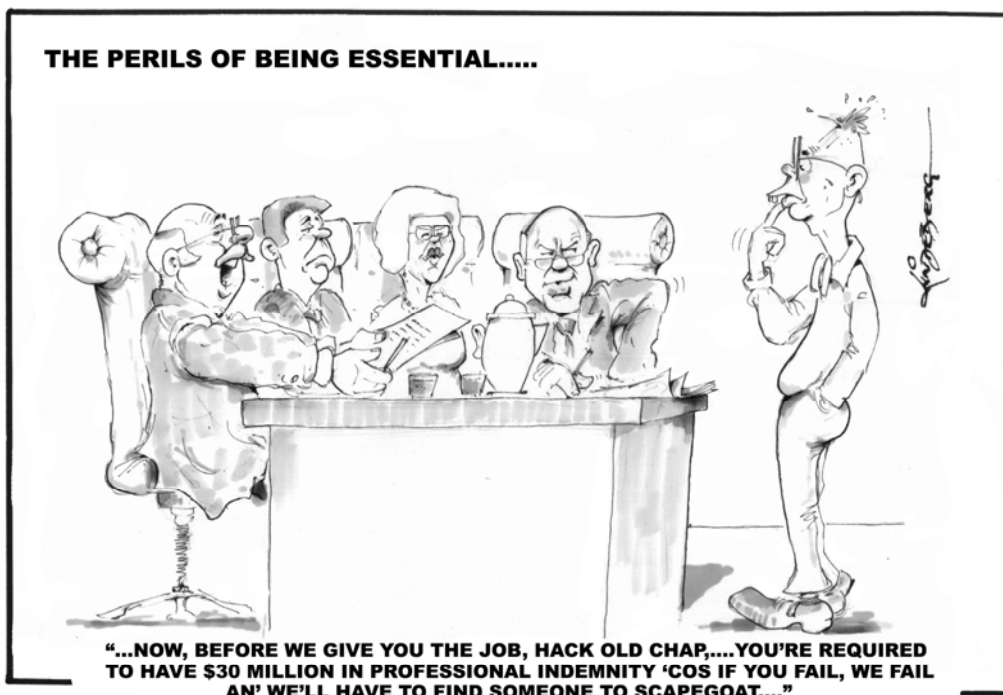
This year’s CACS conference content will include up-to-date coverage on technical and managerial issues associated with information systems security, IT governance and assurance topics. A comprehensive program of social events will complement the conference’s technical program to ensure that delegates enjoy their Oceania CACS 2005 Perth experience. Check out www.isaca-perth.org for more details.

Research Spotlight

Aligning COBIT, ITIL and ISO 17799 for Business Benefit: Management Summary

This management briefing is the result of a joint study initiated by ITGI and the UK Government’s Office of Government Commerce (OGC), in response to the growing significance of best practices to the IT industry and the need for senior business and IT managers to better understand the value of IT best practices and how to implement them. COBIT can be used at the highest level, providing an overall control framework based on an IT process model that generically suits every organisation. There is also a need for detailed standardised practitioner processes. Specific practices and standards such as ITIL and ISO 17799 cover specific areas and can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials.

This publication is a complimentary download available at www.isaca.org/research.





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

Conference Update

24-26 October, 2005 - Oceania CACS - Perth, Western Australia

14-16 November - Network Security Conference & Information Security Management Conference - Amsterdam, The Netherlands

1-2 December - COBIT User Convention - Orlando, Florida, USA

19-22 March 2006 - EuroCACS, London, England

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, go to www.isaca.org/conferences

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.

2005/2006 ISACA Sydney Chapter Board

President	Gladys Rouissi	9378-7874	president@isaca.org.au
Vice President & PD	Johan Pelsler	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	9322-7601	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
Mentoring & CISA	Mike Thompson	9226-1590	cisa@isaca.org.au
Director	Richard Stapleton	9372-0841	director@isaca.org.au
<i>Administration Manager</i>	<i>Helen Gulson</i>	<i>9958-0143</i>	<i>helen.gulson@isaca.org.au</i>