

## Message from the President

Dear readers,

Another year comes to a close and a new year is just around the corner. Everyone is now thinking about Christmas presents, staff lunches, how they got on in their CISA exam, New Year's resolutions. I also believe that this is the time we should look back at our year and see what happened. What did we do? What didn't we do that we could have, or should have done? Was I there for my family? I am achieving my life's objectives, my dreams? This thought process will definitely lead to a lot of soul searching, especially if you're going through a period of uncertainty in your job and where your career is going. I believe that most of you have carried out this thought process and felt that CISA provided you with an opportunity to change direction to something more exciting, to new ventures. And I firmly believe that these people have made an opportunity for themselves and CISA has not let them down.

A number of our members have ventured into new territory irrespective of their background, be it Accountancy, IT, Internal Audit or whatever other professions have decided that IT Auditing was something they wanted to try. We have had a number of members move to new jobs with different responsibilities. During this past year, three of the Big 4 Audit firms in Malta issued vacancies with CISA requirements. I myself, together with Trevor Axiak decided to set up our own company. A bold move, but our experience and knowledge, together with our CISA qualification gave us courage to attempt this move. We believe that qualifications provide credibility to a persons skill sets as noted in their CVs.

I hope that you all find the CISA qualification just as rewarding in your lives and that you say that you are a CISA with pride and that your work also reflects your professional status and standing. Together we are making a name for ourselves such that we have created a market for our unique skills and we must strive to grow this market and to satisfy its requirements with professionalism.

Happy Xmas and the Best New Year to all our members and their family.

Alan Alden,  
President, ISACA MALTA CHAPTER.

## From the Editorial Board

Dear readers,

The 5<sup>th</sup> newsletter issue has at last been issued. We hope you enjoyed reading it and that you will find the information or links to information as beneficial to your profession.

One of the problems that we are faced with every issue of the newsletter is content. The problem is two-way. The first job is for the editorial board to chase some members to submit articles and information. I am sure that many of the members know how to write something on any subject they are knowledgeable about. However the editorial board is always faced with lack of articles.

The second problem faced is about the content itself and the design. The board would like to hear from members on the current design and content of the newsletter. We would appreciate both comments in favour or recommendations how to improve. Without such feedback it is impossible to gauge what value the newsletter is giving to the chapter members.

Therefore it would be highly appreciated if you can drop us a line or two by email to [newsletter@isaca-malta.org](mailto:newsletter@isaca-malta.org). It would be more greatly appreciated if you can include an article or two with your comments.

Finally, on behalf of the editorial board, I would like to wish every reader a Happy Christmas and a joyous New Year. I would also exchange our greetings to your families, friends and co-workers.

Anthony Formosa  
f/Editorial Board



## In this Issue

Message from the President, Research Update, Questions and Answer, Resources, News Snippets, ARTICLE: "To profess or not to profess...is that the question?"

## PLEASE RENEW YOUR ISACA 2007 MEMBERSHIP

The 2007 invoices should have by now been received by all members. Members may renew by remitting the invoice with payment or by paying online on the ISACA web site. Certified members are reminded to renew their certification status and submit the CPE hours together with their renewal.

### Editor

Gordon Micallef

### Contributors

Anthony Formosa

### Published by

ISACA Malta Chapter

For more information about the local chapter contact us on [info@isaca-malta.org](mailto:info@isaca-malta.org)

### **CISA and CISM Exam Highlights**

Registration for the December exam administrations closed with more than 13,300 Certified Information Systems Auditor™ (CISA®) and 2,000 Certified Information Security Manager® (CISM®) exam registrants. Approximately eight weeks after the test date, the official exam results will be mailed to candidates. Additionally, with the candidate's consent to item 25 on the registration form and payment in full, an e-mail containing the candidate's pass/fail status and score will be sent to the address listed in the candidate's profile at the time of the initial release of the results. To ensure the confidentiality of scores, exam results will not be reported by telephone or fax. Candidates should add *certification@isaca.org* to their address book, white list or safe-senders list.

Registration for the June 2007 CISA and CISM exams began the second week of November. Candidates may view or print a copy of the CISA or CISM Bulletin of Information for the June 2007 exams at [www.isaca.org/cisaboi](http://www.isaca.org/cisaboi) and [www.isaca.org/cismboi](http://www.isaca.org/cismboi)

### **CISA and CISM Scoring Change**

ISACA's CISA and CISM certification boards recently approved changing the way exams are scored. To alleviate confusion with the previous scoring method and provide greater clarity, ISACA will use a 200-800 point scale with a passing point of 450, beginning with the June 2007 exam. Using a 200-800 scale will increase the range of scores and also eliminate the perception that the score is a percentage. This scoring method is used by several testing organizations, including the well-respected SAT and GRE exams.

### **Standards Update**

Feedback is sought on the exposure draft for the IS Auditing Guideline titled Configuration Management Process. Please review the draft and provide any comments via the questionnaire posted with the exposure document. All comments received will be carefully considered by the Standards Board. Please submit comments regarding the IS Auditing Guideline on the web site at [www.isaca.org/standardexposure](http://www.isaca.org/standardexposure) or via e-mail to [standards@isaca.org](mailto:standards@isaca.org) no later than 8 January 2007. Please note that CISA/CISM CPE credits are earned for exposure draft review under the category "contributions to the IS audit and control profession" (10-hour annual limitation).

The Standards Board has issued the IS Auditing Guideline G36 Biometric Controls, which becomes effective for IS audits commencing after 1 February 2007.

### **Distance Learning Opportunities**

ISACA is pleased with the member response to the new e-learning opportunity: ISACA e-symposia. The September event had more than 4,000 participants.

The next e-symposium, to be held on 12 December, focuses on security management, and the 30 January 2007 e-symposium will highlight COBIT and its derivatives.

To register for an e-symposium and earn three CPE credits, please visit [www.isaca.e-symposium.com](http://www.isaca.e-symposium.com). If unable to join live and online the day of the event, please log on to [www.isaca.e-symposium.com](http://www.isaca.e-symposium.com) to view the archived programs.

### **Bookstore Update**

New ISACA/IT Governance Institute (ITGI) research and peer-reviewed books are offered in the ISACA Bookstore and include:

- *Security, Audit and Control Features Oracle E-Business Suite: A Technical and Risk Management Guide, 2<sup>nd</sup> Edition\**
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2<sup>nd</sup> Edition\**
- *Audit Procedures 2007*
- *Sarbanes-Oxley Guide for Finance and Information Technology Professionals, 2<sup>nd</sup> Edition*

(\*ISACA/ITGI publication)

Visit the ISACA Bookstore at [www.isaca.org/bookstore](http://www.isaca.org/bookstore) and take advantage of secure online ordering, or see the *Information Systems Control Journal* Bookstore insert for additional information. Contact the Bookstore at [bookstore@isaca.org](mailto:bookstore@isaca.org).

## Q&A

Members are invited to submit their questions to the editorial board at [newsletter@isaca-malta.org](mailto:newsletter@isaca-malta.org). Questions relating to the Malta Chapter in general are also invited. This month's question is being put in by the Editorial Board:

### Question:

Where can I obtain reference material for the CISA & CISM 2007 exams?

### Answer:

#### **CISA Reference Material for 2007 Exams**

([www.isaca.org/cisabooks](http://www.isaca.org/cisabooks))

- CISA Review Manual 2007
- CISA Review Questions, Answers & Explanations Manual 2007 Supplement (100 questions)
- CISA Practice Question Database v7 (825 questions)
- CISA Review Questions, Answers & Explanations Manual 2006 (625 questions)
- CISA Review Questions, Answers & Explanations Manual 2006 Supplement (100 questions)

#### **CISM Reference Material for 2007 Exams**

([www.isaca.org/cismbooks](http://www.isaca.org/cismbooks))

- CISM Review Manual 2007
- CISM Review Questions, Answers & Explanations Manual 2007 (300 questions)
- CISM Review Questions, Answers & Explanations Manual 2007 Supplement (100 questions)
- CISM Practice Question Database v7 (400 questions)

CISA & CISM Bulletin of Information for 2007 exam can be downloaded from <http://www.isaca.org/cisaboi> and <http://www.isaca.org/cismboi> respectively.

## APS Bank Investment Services

*Wide product range*

*Independent professional advice*

*Reduced commission fees*

*Attractive returns*

*Personal attention*

APS Bank Ltd is licensed to conduct Investment Services business by the Malta Financial Services Authority and is enrolled as an Insurance Sub-Agent for Medžesza Valletta Life Assurance Company Limited.



ATTARD • FLORIANA • MOSTA • PAOLA • VALLETTA • GOZO

**The Bank You Want Us To Be**

[www.apsbank.com.mt](http://www.apsbank.com.mt)

## Resources

The links below provide access to various resources on the internet that one may use for research purposes. These resources are compiled and were kindly supplied to us by Dan Swanson who is also the moderator of two yahoo groups. The links provide online resources in support of your IT Audit and IT Security efforts. Content related to Governance, Risk Management, and Internal Audit is provided on occasion. Finally, resources related to leadership and strategy is frequently included. This listserv supports Peter's vision - "The most important contribution management needs to make in the 21st century is to increase the productivity of knowledge work & the knowledge worker." - Peter F. Drucker.

To join Dan's 2 email lists you just need to send two blank emails. Finally, please consider forwarding this invitational email to anyone you believe will want to try it out. To subscribe just send a blank email to these two addresses below:

1) [Dans\\_CCCemails-subscribe@yahoogroups.com](mailto:Dans_CCCemails-subscribe@yahoogroups.com)

2) [Dans\\_SECEmails-subscribe@yahoogroups.com](mailto:Dans_SECEmails-subscribe@yahoogroups.com)

1. The AuditNet News for Auditors - December 2006 Issue (is now available).  
<http://www.auditnet.org/auditnet-l.htm>
2. Dan's Internal Audit Corner – BCP & DR “Thought Leadership”. - This month's audit column is in the right hand column - (towards the bottom of the page).  
<http://www.auditnet.org/auditnet-l.htm>
3. Auditing BCP & DR efforts (The Resource Repository).  
<http://www.auditnet.org/drp.htm>
4. What Should Your Business Continuity Efforts Focus On?  
<http://www.itcinstitute.com/display.aspx?ID=2090>
5. The IT Audit Checklist for Risk Management offers:
  - 80 specific checklist items to help assess your audit-readiness
  - Clarification on what auditors want to see
  - Tips on how to effectively communicate with an auditor
  - Pointers on audit preparation, testing, and reporting<http://www.itcinstitute.com/> Note - a brief registration may be required to download the free ITCI white paper.
6. Two UK based resources newsletters.
  - a) Sentinel Newsletter - Edition 13, 30 August 2006  
[http://www.itgovernance.co.uk/news\\_detail.aspx?news\\_id=51](http://www.itgovernance.co.uk/news_detail.aspx?news_id=51)
  - b) 24743 - Info Sec Newsletter - Edition 8, 24 Aug 2006  
[http://www.itgovernance.co.uk/news\\_detail.aspx?news\\_id=47](http://www.itgovernance.co.uk/news_detail.aspx?news_id=47)
7. This check list is intended as a comprehensive survey of the steps that corporations and other organizations should take to reduce their vulnerability to cyber-attacks.  
[www.ussecurityawareness.org/docs/US-CCU%20Cyber-Security%20Check%20List%202007.pdf](http://www.ussecurityawareness.org/docs/US-CCU%20Cyber-Security%20Check%20List%202007.pdf)
8. Create a Winning Strategy for Your Awareness Program.  
Awareness programs are the cheapest way to prevent costly problems, but the security message can be easy to ignore. CSOs and CISOs share their strategies for spreading the good word. - by Lew McCreary.  
[www.csoonline.com/read/110106/fea\\_awareness.html](http://www.csoonline.com/read/110106/fea_awareness.html)
9. "Pass It On". (a simple message for this one - i.e. "share" the tips).  
Valuable security tips and awareness materials.  
<http://www2.csoonline.com/passiton/>
10. November's Tone at the Top issue - (How Vulnerable Is Your Information Technology) is at:  
<http://www.theiia.org/download.cfm?file=52803>
11. Insider Risk Management Audit Guide.  
[http://searchsecurity.techtarget.com/generic/0,295582,sid14\\_gci1213412,00.html](http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1213412,00.html)
12. Measurement & Metrics Guide  
<http://www.oceg.org/viewing/ItemView.aspx?shortcut=MMG>

## *Snippets From The International Info Sec Online Media*

### **EU Legislation Would Force Data Security Breach Disclosure**

European Union legislation due to go into effect in late 2007 would require organizations that experience data security breaches to notify regulators and customers if the breach could expose customer data.

<http://www.vnunet.com/computing/analysis/2169875/telecoms-providers-reveal>

<http://www.net-security.org/secworld.php?id=4450>

### **Novel Security Technologies with Real World Use**

In this article about novel approaches to security Goldman Sachs is testing digital rights software to prevent browsing, printing or changing financial information and the US Navy is working on an authentication system that doesn't require passwords.

<http://www.networkworld.com/news/2006/112706-online-security.html?page=1>

### **Media exec charged with computer break-in**

He broke into corporate network after dismissal, prosecutors say - A former Source Media Inc. executive was charged with hacking into the company's computer system three years after he was dismissed, and tipping off employees whose jobs were in jeopardy, prosecutors said.

<http://www.msnbc.msn.com/id/15739188/>

### **Man used MP3 player to hack ATMs**

Parsons plugged his MP3 player into the back of free standing cash machines and was able to use it to read data about customers' cards. That data could then be used to 'clone' cards and use them for bogus purchases.

[http://www.theregister.co.uk/2006/11/18/mp3\\_player\\_atm\\_hack/print.html](http://www.theregister.co.uk/2006/11/18/mp3_player_atm_hack/print.html)

### **Guidelines for Financial Institution End-User Authentication May Not be Strong Enough**

IT analysts and managers are concerned that federal guidelines for end-user authentication do not go far enough to secure customer data. While the "strong authentication" measures recommended by the Federal Financial Institutions Examination Council (FFIEC) are a step in the right direction, there are other vectors through which financial data security could be breached. The FFIEC guidelines are designed to bolster single-factor authentication; some attackers have already developed methods for circumventing the one-time password measures some banks have implemented in their two-factor authentication schemes. Financial institutions may also want to consider transaction-level controls and real-time online account activity monitoring.

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=274881&taxonomyId=17&intsrc=kc\\_top](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=274881&taxonomyId=17&intsrc=kc_top)

### **Phishers Hit VoIP**

Voice over Internet Protocol (VoIP) has become the latest vector of attack for phishers. Some attacks come in the form of emails asking the recipients to call a certain number to verify sensitive account data; the call is recorded. Other attacks come as phone calls in which the caller already knows the recipient's credit card number and asks for the security code for verification purposes.

[http://www.usatoday.com/money/industries/technology/2006-11-26-phishing-usat\\_x.htm?csp=34](http://www.usatoday.com/money/industries/technology/2006-11-26-phishing-usat_x.htm?csp=34)

### **Panel Condemns SWIFT Actions**

The Article 29 Working Party, a group looking into the issue of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) sharing transaction information with the US says that SWIFT must inform clients that their personal financial information could be given to US authorities. The group found that EU banks using SWIFT to conduct their financial transactions "share culpability" for the data exposure. The group also said that "the ... systematic, ... long-term transfer of personal data by SWIFT to the UST (US Treasury) in a confidential, non-transparent ... manner for years without effective legal grounds and without the possibility of independent control by public data protection supervisory authorities" violates EU data protection laws. The panel recommends that SWIFT stop violating the laws or face sanctions.

<http://www.independent.com.mt/news.asp?newsitemid=42551>

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005387&source=rss\\_topic17](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005387&source=rss_topic17)

# To profess or not to profess...is that the question?

By Melody Morgan-Busher

Members of ISACA are subject to the published “Code of Professional Ethics”. Do we all know the content of this code? How does the code fit the local context and how relevant is it to our day-to-day work?? And how much can we read between the lines or ignore.

I believe that one of the benefits of the local ISACA chapter is the chance to discuss non-technical, but important aspects of the ICT industry with one’s peers. How to set standards, read regulations and make mission statements come true are all areas where we may benefit from collective experience. The Malta Chapter is a select band and it is hoped that there will be more opportunities in future for members to meet and exchange views.

Those who sit for the CISA and CISM examinations are trained in “best practice” (according to ISACA) in regard to information systems auditing and information systems security management. At work, we must all make assumptions about what is “normal practice” yet may lack any independent means to check our opinions. We may lack the confidence to challenge homegrown “normal practice” even when it deviates significantly from received “best practice”. In my view, there is often knowledge of what should be done, but a shortage of experience of how it can be achieved and the willingness to hold out for it.

Below is a brief review of the ISACA Code of Professional Ethics as these principles are worthy of debate and consideration – available online under the ISACA Main Menu “Members & Leaders”.

Members are to:

*1. Support the implementation of, and encourage compliance with appropriate standards, procedures and controls for information systems*

It follows that all ISACA members are 100% content with their employers’ controls and adherence to procedure! If not, what action is appropriate and effective? How can a CISA employee use their training to convince their boss to make improvements? I liked Duncan Hart’s recent talk in which he spoke of recognising “near misses” and believe that this may offer a positive way to highlight areas of Information Systems weakness without breaking anything!

*2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices*

We may consider ourselves objective, but of course, we can never achieve this ideal as our outlook is influenced by our personal history and our environment. However “due diligence and professional care” should ensure that we limit our bias and declare any conflicts of interest. The meaning of the word “professional” is worthy of a debate all on its own – some people see it as drawing a line around what one is liable for; others see it as bringing liability for all consequences.

*3. Serve the interest of the stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession*

The stakeholders would be those who own and manage the Information Systems under audit/subject to control I assume. They may also include any data subjects whose information is made available to the auditor/information security manager and other third parties depending on the case. This clause seems to cut both ways – the ISACA member must neither benefit neither the stakeholder nor himself by abuse of his privileged position.

*4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for benefit or released to inappropriate parties.*

This principle is simply stated, but less easy to implement when one takes verbal disclosure into account in the highly networked context of Malta. The “need to know” concept is a useful check; assigning ownership of information assets in larger organisations may also help determine what is legitimate access as there will be a clearly designated person to refer to in every decision.

*5. Maintain competency in their respective fields and agree to undertake only those activities which they can reasonably expect to complete with professional competence*

We all try to stay current and we probably all feel insecure due to the pace of change – but take heart, there is nothing new about this feeling. The IT industry is celebrating its first half century yet is still considered to be an emerging field. Looking at books from 20 and 30 years ago, the authors were lamenting the rate of IT change then! Malta has plenty of talent, but perhaps not as much as it needs; over-commitment of staff is more likely to cause poor performance locally than their individual skills. Being able to delegate and prioritise work may be an important factor in professional success.

6. Inform appropriate parties of the results of work performed; revealing all significant facts to them.

This appears simple and self-evident yet the provision of a comprehensive audit report and supporting documentation to the relevant stakeholders is a vital part of a control review process. It will allow subsequent audits to be accurately compared and will provide a reference point for other decisions. It is not the most glamorous part of the job, but is where the quality of analysis and method will show. It is also the part where social and political pressure is most likely to be felt; including a finding in a report may make or break some-one else's fortune whilst reporting it verbally may be enough to clear one's conscience. What to do? Proportionality and materiality are relevant considerations, but the auditor/security manager must empower his superiors to make informed decisions.

7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

I guess this is a ban on making a black art out of information systems security management and a plea to "recruit more members"! What I am left wondering is if ISACA have actually disciplined any one of their 58,000+ membership for breach of this Code of Professional Ethics... Or is it enough that we profess to follow the code?

Your comments on the above are invited and welcome – please email feedback to the Editor at [newsletter@isaca-malta.org](mailto:newsletter@isaca-malta.org).



EuroCACS  
18-21 March 2007  
Vienna, Austria



ISACA proudly announces its European Computer Audit, Control and Security (EuroCACS) conference where IT assurance, security and governance professionals meet to discuss and debate today's most important issues and challenges. This unique event focuses on the latest strategies to address business, managerial, operational, auditing and security challenges associated with information technology and information systems. Conference streams include IT governance, IT audit, information security, and risk management and compliance. For more information and to register, please visit [www.isaca.org/eurocacs](http://www.isaca.org/eurocacs)

**Notice**

Any member intending to attend the EuroCACS conference and workshops due to be held in Vienna, Austria, kindly contact the local chapter at [administration@isaca-malta.org](mailto:administration@isaca-malta.org).

**2006-2007 Conference/Training Week Calendar**

	ISACA Training Week	COBIT User Convention	Information Security Conference	ISACA Training Week	Euro CACS <sup>sm</sup>	North America CACS <sup>sm</sup>	ISACA Training Week	International Conference	Oceania CACS <sup>sm</sup>
<b>Dates</b>	4-8 December 2006	18-19 January 2007	5-7 February 2007	26 February-2 March 2007	18-21 March 2007	22-26 April 2007	7-11 May 2007	22-25 July 2007	9-12 September 2007
<b>Location</b>	Orlando, Florida, USA	Pasadena, California, USA	Panama City, Panama	Washington DC, USA	Vienna, Austria	Grapevine, Texas, USA	Denver, Colorado, USA	Singapore	Auckland, New Zealand
<b>CPE Hours</b>	38	13	21	38	40	44	38	TBA	TBA

The *Information Systems Control Journal* is provided free to ISACA members and is available to others by subscription. Visit this area for information on subscriptions, advertising, and becoming an author for the *Journal* or to fill out a Reader Survey or CPE Quiz online.

<http://www.isaca.org/currentissue>



Volume 6, 2006

### Membership Benefits

#### COBIT Mappings:

1: ITGI has released a number of mappings between COBIT and various standards. The COBIT Mappings are available exclusively to ISACA members. Most recently, ITGI has released mappings to PRINCE2, ISO 17799:2005 and ITIL.

2: Available at [www.isaca.org/deliverables](http://www.isaca.org/deliverables)

#### Application Forms

Membership application form is available from the ISACA website on [http://www.isaca.org/Content/NavigationMenu/About\\_ISACA/Membership/membership.pdf](http://www.isaca.org/Content/NavigationMenu/About_ISACA/Membership/membership.pdf)

Special offer applies for verified full-time students

[http://www.isaca.org/Content/NavigationMenu/Students\\_and\\_Educators/Join1/Student\\_Membership\\_Information.htm](http://www.isaca.org/Content/NavigationMenu/Students_and_Educators/Join1/Student_Membership_Information.htm)

CISA® and CISM® certification -  
the only thing missing is... U

#### Chapter Bylaws

Download the Chapter Bylaws from [www.isaca-malta.org](http://www.isaca-malta.org)



#### Notice To Members

ISACA members are requested to update their details by logging on to "My ISACA" at [www.isaca.org](http://www.isaca.org).

### Chapter Board Composition

The board composition for the year 2006/2007 is as follows:

- President - Alan J. Alden [president@isca-malta.org](mailto:president@isca-malta.org)
- V.President - Gordon Micallef [info@isaca-malta.org](mailto:info@isaca-malta.org)
- Secretary - Anthony Formosa [administration@isaca-malta.org](mailto:administration@isaca-malta.org)
- Treasurer - Alexander Camilleri [treasurer@isaca-malta.org](mailto:treasurer@isaca-malta.org)
  
- Members -
  - Membership Coordinator – Kevin Fenech [membership@isaca-malta.org](mailto:membership@isaca-malta.org)
  - CISA/CISM Coordinator – Kenneth Ciantar [cisa@isaca-malta.org](mailto:cisa@isaca-malta.org)
  - Academic Relations Coordinator – Dr Robert Cachia [academic@isaca-malta.org](mailto:academic@isaca-malta.org)
  - Media Relations – Christopher Azzopardi [media@isaca-malta.org](mailto:media@isaca-malta.org)
  - Education Coordinator - Charles Theuma
  - BCS Liason – Melody Morgan Busher



**CISA**, the Certified Information Systems Auditor is ISACA's cornerstone certification. Since 1978, the CISA exam has measured excellence in the area of IS auditing, control and security. CISA has grown to be globally recognized and adopted worldwide as a symbol of achievement. The CISA certification has been earned by more than 35,000 professionals since inception. For more information refer to the following link [www.isaca.org/cisa](http://www.isaca.org/cisa).

**CISM**, the Certified Information Security Manager is ISACA's groundbreaking credential earned by over 5,100 professionals in its first two years. It is for the individual who must maintain a view of the "big picture" by managing, designing, overseeing and assessing an enterprise's information security. For more information refer to the following link [www.isaca.org/cism](http://www.isaca.org/cism).

You are encouraged to circulate the PDF version of this newsletter to anyone provided that it remains unchanged and intact (including this copyright notice), is not embedded in any other product or service and is provided free of charge.