Information Systems Audit and Control Association

SAN FRANCISCO CHAPTER LOCAL AREA NETWORK

FIRST QUARTER 2000

Winner of the 1999 ISACA International Newsletter Contest – Best Chapter Newsletter for Large Chapters in North America

PRESIDENT'S MESSAGE

Carol Hopkins
President

2000 Luncheon and Afternoon Session Topics

January
Career Development

February
IS Audit Best Practices – Session I

March
Secure Network Communications

April
Audit, Control and Security of E-Commerce

May
Audit, Control and Security of Windows NT

June
Audit, Control and Security of UNIX

July
Auditing Rapid Application Development

August
Assessing Your Organization's Privacy Policy

September
IS Audit Best Practices – Session II

October
Best Practices for Business Continuity and Disaster Planning

November
Best Practices for Intrusion Detection

December
Audit, Control and Security of Oracle

All of our year 2000 project plans have been developed. The membership database has been updated with your correct e-mail addresses, our year 2000 Educational Program has been completed and the Web site has been updated to reflect the new educational line-up. We are ready for Y2K.

Can you believe that Y2K is here? A new millennium – a great opportunity for change. As this year progresses many new opportunities will be presented and we will have to be proactive to capture the benefits that they present. I hope that each of you takes some time to reflect on what you have achieved in your life and where you want to take your life in the new millennium.

One fabulous opportunity for you to embark on in 2000 is to become more active in the San Francisco ISACA Chapter – your Chapter. You may be receiving a call from the committee chairs to request your personal support for our year 2000 projects. If you can give a small part of your busy life to assist us in making this year a success, we all will benefit from your generosity.

I want to thank all of the members who have already sent in their membership dues for 2000. As I mentioned in the November bulletin, prompt payment of your dues is critical to our organization's success. Also, there is a $50.00 prize available (refer to your November Bulletin for more details).

Our first sponsor for 2000 is Valacon, Inc. On behalf of the Board of Directors, I would like to thank Sandy Geffner, President of Valacon, for his continued support for our Chapter. Sandy will be our speaker at our first meeting in 2000. His topic will be career planning. We thought this would be a good way to kick-off the new millennium. It is very important for each of us to take our career into our own hands.

While on the subject of education, our monthly education session's format and pricing will change in 2000. Each month we will cover only one topic (as opposed to having separate topics for the luncheon and afternoon seminar). The luncheon session will be a high-level overview of the topic. The afternoon session will be a more in-depth look at the same subject. The new schedule and costs are as follows:

Schedule and Costs for 2000 Luncheon and Afternoon Sessions

Luncheon Session Schedule

11:30 AM – 2:00 PM
11:30 AM Registration
11:45 AM Lunch
12:30 PM Presentation

Afternoon Session Schedule

2:15 PM – 4:30 PM (or later depending on the topic and presenter)

Member Fees

Luncheon Only – $30.00
Both Luncheon and Afternoon Session – $40.00

Non-Member Fees

Luncheon Only – $40.00
Both Luncheon and Afternoon Session – $60.00

Full-time Student Fees

Luncheon Only – $10.00
Both Luncheon and Afternoon Session – $15.00

We are Y2K-OK and still getting better and better everyday in every way!

Carol Hopkins, CISA, President

REDEFINING INTERNAL AUDIT

By Richard Tuck, CES, CPC, CIPC

Richard Tuck, CES, CPC, CIPC is the President and Founder of Lander International, the world's largest IS audit and resource center. He is a former President of the San Francisco Chapter of ISACA and currently serves on the Advisory Board.

Todd Weinman and I had the privilege last week of making a presentation to one of Northern California's most prestigious audit committees. The Chief Auditor of this organization had invited us to give an overview of the changing role of internal audit in many of the world's best organizations. We were expecting a small group since it was just the members of this company's audit committee convened for their semi-annual meeting with the internal audit department to review findings and discuss next year's budget. To our surprise the room was filled with close to 40 audience members. When word had gotten out about potential changes in the direction internal audit was planning to take for the future, suddenly the CEO, CFO and CIO were interested enough to attend.

The cornerstone of our presentation was the new definition of Internal Audit that the Institute of Internal Auditors unveiled in June of this year. As I went over the points of the new, much broadened definition, I could see some people in the room growing uncomfortable. According to the IIA, as of June 1999, internal auditing is "an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." I pointed out during the meeting that the new definition was approved unanimously by the IIA Board of Directors, thus it is a compromise definition. Many very progressive organizations preferred a far broader definition, but, at a minimum, the board members agreed that internal audit is now officially in the consulting business.

Todd Weinman gave the group many examples of how Northern California audit departments have already developed into value-added partners actively involved with assisting business units achieve their goals. The executive officers in the audience began to smile and ask questions about how the changes came about. The auditors in the audience were relieved that the questions asked by the executives were friendly and demonstrated they were beginning to buy into the new, more cooperative approach.

One of the audit committee members, an attorney, asked how the auditors should be compensated when they were actively involved as problem solvers for the entire organization. I became very popular with the auditors when I gave examples of auditors receiving bonuses based on their contributions.

Another audit committee member asked my opinion about adding a compliance unit to the existing audit group to ensure that new regulations and laws were being properly followed, an idea that brought frowns to many faces in the room. I reminded the questioner that the ultimate responsibility for compliance rests not with auditors but with senior management. Todd chimed in with instances where business units have hired their own experienced auditors to do pre-audits before the regulators show up to do their annual inspections, and these hired pre-auditors worked totally independent of the internal audit departments.

The feedback after the session has been heartening. Immediately following our presentation, the Chief Auditor took over the meeting and outlined his plans for the department this next year. Apparently the audit committee was open-minded and receptive to hearing about a more consultative approach. The CEO and other executives now seem very interested in the expanding involvement of the audit department in helping the entire organization capture its goals.

Over the last two decades I have spoken at hundreds of conferences and chapter meetings of the IIA and ISACA about the evolving role of the audit profession. I have felt most of the time that the auditors themselves were interested in becoming more consulting-oriented. The obstacle standing in the way of such a move towards consulting was usually perceived to be either the audit committee and/or senior management. I think the time has finally arrived. As I pointed out to the audit committee last week, the IIA is a very conservative organization. For the IIA to unanimously embrace the new, enlightened definition of internal audit is a major break through. Now it's time for individual departments to start living up to the new definition.

THE WORLD WIDE WEB

Lance Turcato
Communications Coordination and Web Master

The Oracle Technology Network

http://technet.oracle.com/index.shtml

Computer and Network Security Reference Index

http://www.telstra.com.au/info/security.html
This site contains a list of links to information sources on network and computer security.

Windows NT Frequently Asked Questions

http://www.ntfaq.com/

NTBUGTRAQ.COM

http://www.ntbugtraq.com/
NTBugtraq is a mailing list for the discussion of security exploits and security bugs in Windows NT and its related applications.

NTSecurity.Com

http://www.ntsecurity.com/

Unix Guru Universe

http://www.ugu.com/
This site provides you with a search facility to find almost anything relating to UNIX (Company/Vendors Names, commands, types of hardware, platforms, and more).

RSA Security Welcomes New California E-Commerce Law

http://www.rsasecurity.com/news/pr/990924.html
RSA Security welcomes new California e-commerce law pioneering legislation based on RSA Security technology sets standard to validate most electronic transactions.

Certisource

http://www.certisource.com/index.asp
One stop shopping for technical education and services.

International Information Systems Security Certification Consortium, Inc.

http://www.isc2.org/index.html

Job Opportunities and Links To Recruiters

http://www.sfisaca.org/resources/jobs.htm

Links to Career Planning Information

http://www.sfisaca.org/resources/career.htm

www.sfisaca.org

Learn about the San Francisco Chapter

Learn about the CISA certification

Test your skills with our CISA sample test questions

Complete our member survey

Access information regarding ISACA international

Access information regarding our Student Chapters

Register for monthly meetings

Register for seminars

Access information regarding ISACA conferences

Register for the CISA review course

Access our Chapter newsletters and monthly bulletins

Update your membership information (address, phone, E-mail)

Access IS audit, control and security resources

Research employment opportunities

Join a Chapter committee

Learn how you can join ISACA – understand the benefits

Contact Chapter Officers and Directors

Access these and other sites from the Chapter's Web site at www.sfisaca.org/resources/index.htm

To submit an article, suggest Web sites, or to contribute other items of interest for inclusion in future newsletters, please contact our Communications Committee Chair and Web Master, Lance M. Turcato, CPA, CISA at 415/636-8158 or lance.turcato@schwab.com.

MEMBERSHIP

Hector Massa
Committee Chairperson

The membership count for the San Francisco Chapter as of November 10, 1999, stands at 353 members. Please join me and the SF ISACA Board in welcoming these Chapter members.

Richard J. Angus
Wells Fargo Bank

Brad D. Chin, CISA, CPA
Ernst & Young LLP
Reinstated Member

Michael J. Cronin
Comptroller of the Currency

Pal Danyi, CISA
Ernst & Young LLP
Transfer from Budapest Chapter

William Dei
Federal Reserve Bank
of San Francisco

Christopher D. Hansell,
CPA, CA
PricewaterhouseCoopers LLP

Jeff C. Lai
Oakland, CA
Transfer from
Hong Kong Chapter

Kenneth K.C. Lau, CISA
VEBA Electronics
Transfer from
Los Angeles Chapter

Viktoria Lewis, CIA, CISA
Technology Credit Union

Richard A. Loving Jr. CPA
Ernst & Young LLP
Transfer from
Philadelphia Chapter

Andrew H.H. Ng, CPA
Deluxe Corporation
Transfer from
Minnesota Chapter

Ophelia Garcia Nicandro
Federal Reserve Bank
of San Francisco

Juanita M. Ostrander
State Compensation Ins. Fund

Hector O. Rivera
FEMA
Reinstated Member

Hugh Rosengarten, CISA, CA
Ernst & Young LLP
Transfer from
South Africa Chapter

Maria J. Shaw, CA, CISA
Deloitte & Touche LLP
Transfer from London Chapter

Angela M. Stewart
U.S. Department of Labor
Office of Inspector General
Transfer from National
Capital Area Chapter

Anna G. Tchernina
Deloitte & Touche LLP

Edward S. Thompson
State of California

John C. Tryon, CPA,
CIA, CISA
Kaiser Permanente

Bill D. Vourthis
Redwood City, CA

Stuart R. White
Deloitte & Touche LLP

Mary B. Wolverton
State Compensation Ins. Fund

Tammala D. Woodrum
Genetech, Inc.

Jason Z. Xie
Ernst & Young LLP

Ronald W. Yu
Deloitte & Touche LLP
Transfer from
Puget Sound Chapter

Jeff Zhou
Deloitte & Touche LLP

Member Milestones

Join the Board of Directors in saluting the following long-term Chapter members:

Members for over 20 Years

Robert Abbott
Douglas Webb
Hector Massa
Arnold Dito
David Durst
John Sheehan
Richard Tuck
Charles Cresson-Wood

Members for over 15 Years

William Davidson
Robert Kimball
Joel Lesser
William Martin
Bruce L. Reid
Kathleen Williams
Ronald Rasch
Kerry G. Elms
Harry Lew
Allen Martin
William T. Tener
Frank Yee
Jerry K. Hill
Kathrerine Ullman

Members for over 10 Years

Ben H. Choi
Marcus A. Jung
Nancy Weisbrook
Eugene Menning Jr.
Paley Pang
Vickie Smith
Guy Anderson
Adam F. Levine
Robert C. Motts
Sharon Tatehara
Ann Y. Lee
I-MEI Chen
Ralph Nefdt

Please contact our Membership Committee Chairperson if you have questions regarding the above information (Hector Massa: hlmsa@aol.com). Keep the Chapter informed of milestones you achieve in your career. Send an overview of your accomplishments and career changes to Lance Turcato, Communications Committee Chair (lance.turcato@schwab.com).

WHAT'S HAPPENING TO THE IS AUDIT JOB MARKET?

By Gerry Meyers

Gerry is owner of Gerry Meyers and Associates, Inc. and IS Audit Consultants. He is a Past President of the Chicago ISACA and the Central Ohio ISACA Chapters; he was also International President of ISACA and President of the ISACA Foundation for Education and Research.

Supply and Demand

Staff IS Auditors with at least one to two years experience and senior IS Auditors are still very much in demand. The demand for IS Audit Managers has slackened in some locations.

Trends – Career Moves

Many IS Auditors changed jobs this year to improve their career paths or to raise their take-home pay. Why can't companies hold their good people? No upward movement possibilities and/or small raises seem to be the major reasons. Too many companies flattened out their staffs eliminating middle management positions. Many Supervisors' and Managers' positions were wiped out. The remaining Senior Managers found themselves running audits and directly supervising large staffs. Many of these Managers became stretched out and were ineffective both in handling the audits and trying to communicate with so many staff people. The staff people also became frustrated with no opportunities to advance, mass micro managing, and small raises. When you consider the costs of obtaining good staff such as recruiting fees, relocations, signing bonuses, temporary housing allowances, etc., one should stop and consider how to retain these valuable people assets. Add to the equation the costs of training people and you soon realize there is a lot of money and time invested in staff who will probably quit after 2 years and might very well end up on a competitors' audit staff. (Fortunately, some companies are waking up and reestablishing middle staff positions with higher pay grades. Let's hope this trend continues!)

Trends – Outsourcing

The big CPA firms continue to aggressively pursue new business. Some continue to bid to not only outsource the IS Audit function, but the entire Internal Audit Department as well. We have seen two interesting trends. First, some companies have decided not to continue outsourcing or cosourcing, but to discontinue the services of the CPA firm and to revert back to their own salaried staffs. Secondly, some CPA Managers in one location have been notified that their services will no longer be needed after a certain date. We can only speculate on the reasons, but we feel their firm either did not meet their goals or they did not hire the right folks during the past two years while expanding their staffs to gear up for the additional coverage needed.

Best Wishes and see you next Quarter!

INFORMATION SECURITY AS WE ENTER THE NEW MILLENNIUM

A Conversation with Charles Cresson Wood

by Todd Weinman

In addition to being on our Board of Directors as 2nd Vice President and the Education Chair, Todd Weinman is an executive recruiter for Lander International, the world's largest full service IS audit resource center. Todd enjoys visiting audit, information security, and consulting departments all over Northern California, and he is in contact on a daily basis with scores of directors, managers and staff level professionals from around the region.

He is also a frequent speaker for ISACA, the IIA and local universities. Todd is a graduate of UC Berkeley and worked in public accounting prior to joining Lander International.

Todd was recently selected as the CAPC 1999 Consultant of the Year for the state of California.

Charles Cresson Wood is general manager of Baseline Software, a firm that sells the books that he has written, including the highly acclaimed *Information Security Policies Made Easy*. He is also a management consultant who performs risk analyses, who develops information security architectures, and who prepares organizational infrastructure documents such as policy statements.

Charles has passed the CPA exam, and he is also a CISSP and a CISA. Charles has an MBA in financial information systems, a MS in computer science, and a BSE in accounting. A long time supporter of the ISACA SF chapter, he also has given several speeches to the chapter over the years.

To most individuals in the world of information security and information systems audit, Charles Cresson Wood is a household name. For over 20 years he has been one of the world's foremost authorities on information security and he is a recipient of the Computer Security Institute's Lifetime Achievement award. Charles Cresson Wood is usually the first name that comes to mind when Fortune 500 companies experience a major breach in security, or when growing companies are considering starting an information security function for the first time. He is a prolific author, having written over 200 articles and five books, including the vastly popular, *Information Security Policies Made Easy*.

Who better, then, to consult with on the current state of information security as we enter the new millennium. The following is a transcript of our recent conversation.

What are some of the major changes and developments in information security as we enter the new millennium?

I have seen a number of dramatic changes in the field of information security over the past several years, and I see continued rapid change in the future. Perhaps the biggest shift has been that in the past, information security has been viewed as a policing organization, as overhead, and as a necessary evil. More and more, however, we find perceptions of information security changing from that of process stoppers to process enablers. For example, the modern workplace with mobile workers and remote access would not be possible without dynamic passwords, VPNs and other information security technology. In fact, not only is information security now being viewed as important to the business, but in many organizations, the information security function is regarded as a key resource that adds value and contributes to the competitive advantage of the organization. Certainly one way this takes place is by a good information security function mitigating risk to the organization, but it goes beyond that. With the onset of e-commerce, the stakes of a secured information security environment increase dramatically. Many consumers will make purchasing decisions over the Internet based upon their confidence level of the organizations ability to protect the privacy of their personal data, and any kind of security breech that would hit the newspapers would severely undermine that confidence. Moreover, as the modern organization increasingly becomes a complex web of disparate entities (i.e. contractors, temps, joint ventures, strategic alliances, extranets with third parties) the information security function can become the common thread the weaves all of these different participants together.

There are several indicators that demonstrate the increasingly prominent role of information security. First, as information security is looked upon more and more as a key management resource within the company, we find an increasing number of information security managers and directors with VP and even SVP recognition within their organizations. Similarly, we find the average percentage of workforce within a given company dedicated to information security is steadily and dramatically rising, including a 64% increase since last year and a whopping 300% increase since 1989. These increases outpaced the increases in IS Audit (49% over last year) and outpaced the increases in Information Technology Services (8% over last year).

The changing nature of the information security function can also be found in the profile of the typical information security professional. Years ago, when information security was confined to the glass house, the field was primarily populated by programmers and super-techies with advanced degrees in computer science. The new profile would place an increasing emphasis on people skills and communication skills, as well as overall business savvy. Today's information security professionals need to be able to traverse complex political minefields and to have a sound grasp of the business itself.

What is the greatest challenge facing information security functions today?

Foremost among the many challenges is the issue of coordination. The information security function must make sense of complex organizational structures. It is increasingly becoming a coordination activity in a multi-dependent business environment. It brings together the work of different departments in the organization such as quality assurance, internal audit, information services, risk management and human resources, sometimes coordinating, sometimes mediating, and sometimes just tying to make sense of the mind-boggling array of disparate and often conflicting information. Information security allows for the participation of contractors, outside consultants, Internet connectivity, Intranets and strategic alliances. None of these would be possible without information security. The information security manager provides the "rules of engagement" to allow all of these parties to work together by providing sound security architecture and clear policies and standards.

A second challenge of the modern information security function is to keep up with new scenarios created by the changing business environment and proactively develop policy to address these situations. Allow me to share an example. There was recently a situation where a government employee in the Pacific Northwest was caught downloading pornography from the Internet and subsequently fired. The employee then countered with a lawsuit indicating that management never conveyed to him that this was inappropriate behavior for the workplace. Because there was no standard or policy regarding the downloading of pornography from the Internet, the employee was reinstated with back-pay.

A third challenge facing today's information security departments is the shortage of skilled personnel. In fact, I would go so far to say that skills and staffing, or lack thereof, is the biggest obstacle to executing Internet business strategy. We currently have a gap. Companies want trained people but they do not want to train them. So if people are going to get the necessary training, they must often do it themselves using their own money. This is an incredibly complex field with a need for ongoing training. Organizations like ISACA and ISSA can be a means of obtaining some of that knowledge and skills. I think we will also continue to see many IS auditors successfully transition into information security. They are great candidates for it. They have compatible control perspectives and they understand the politics surrounding information security.

A fourth challenge, one that is lessening in many organizations, is getting peoples' attitudes to change so that they see information security as a central part of the business and a provider of value as opposed to a problem to be dealt with. Traditionally, information security was viewed as a defensive mechanism to prevent bad things from happening. These included things such as detecting computer viruses, preventing the loss or theft of critical or proprietary data, and keeping the organization out of the headlines by preventing incidents of hacking. While these are still considered important goals of the information security function, the challenge is to show how information security can be a proactive force for positive change to the organization. Information security can add value in a litany of ways. Because information security specialists have a view of the entire organization, it can play a proactive role in making recommendations that improve communication and efficiency; for example, VPNs allow leased lines to be eliminated and replaced by Internet connections, thus saving money for the organization and allowing for more communication options. Certainly, in the computer industry, or in companies involved with e-commerce, a strong reputation in the area of information security can actually help sell the product. One example of this is Aetna Insurance Company. They have taken a stand to restrict access to policyholders' private information to a greater extent than other insurance companies. In this way, information security becomes a fundamental part of their marketing concept that has resulted in additional sales and revenue.

Senior management has traditionally evaluated information security and its subsequent funding by using a cost/benefit analysis. But this narrow detailed approach fails to account for many of the ways that information security can increase competitive advantage. It is an inferior method of evaluating the value of information security. The information security manager/director needs to be proactive, then, first in providing additional value and benefit to the organization, and second to make certain that senior management is aware of these contributions.

Finally, I see a fundamental challenge with information security, which at the same time is part of what makes it such a stimulating area in which to work. You may be familiar with Metcalfe's Law which states that the value of a network increases exponentially as the number of users increases, but the costs increase only linearly. This is the concept upon which telephones, networks, client/server and certainly the Internet is predicated. It is also the reason so many organizations are forging new partnerships and alliances, such as Amazon.com's Affinity program.

The challenge of Metcalfe's Law for the information security function, then, is that it flies directly in the face of the traditional information security concept of information on a "need to know" basis. Consequently, there is a constant tension between the benefits of a secured computing environment versus the cost-effectiveness of business functionality. The challenge then is for information security functions to find the right balance between these two and other competing objectives. Information security needs to look for and mediate acceptable compromises to competing objectives within the organization. This is why information security is becoming an increasingly analytical endeavor.

Where, ideally, should the information security function be located within a company, or does it vary from organization to organization?

It varies a lot. Most information security functions report to the CIO or another IT function. However, there is an inherent conflict of interest here. Objectives such as system performance and ease of use are likely to win out over security. What happens when the Information Security manager has to go head-to-head with other people in IT? Security usually loses. Because of this conflict, my preference is for the information security function to be situated within Risk Management, which shares the integrated risk management view found in progressive information security groups. Risk Management also has excellent contact with top management and is supportive of contingency planning efforts.

What are the most neglected elements of information security functions that you see today?

Rather than approaching the question from the standpoint of neglect, let me speak to some of the most important considerations for the information security function. Certainly one of the primary roles is to disseminate training and awareness information throughout the organization. A company can be technically top notch from an information security standpoint, yet if it has not been successful in promoting awareness of the importance of information security to each of the workers, it remains extremely vulnerable.

Another important facet of the information security function is to insure that the information security function is integrated with the business and that it supports the business. What I mean here is that today's business environment often necessitates making difficult choices. Information security's recommendations need to be informed by the specific circumstances of the business. There are times where the information security function can be overly zealous in its recommendations in a way that negatively impacts the business. A firm understanding of the business, then, is essential to balancing sound information security with business functionality.

I would also cite sound information security architecture, clear and meaningful policy and standards as being vital to the success of an information security function, as is the need to have enough qualified people on hand to do the work. It is also important to remember, however, that there is no one size fits all approach. For example, the needs of information security in the military would differ radically from the needs of a retail store. Each organization must prepare its own policy and architecture.

For someone contemplating a move into the information security function, what should they keep in mind? What personal characteristics are important to success in the field?

First and foremost, they need to acknowledge the unique realities of the position. There is not a lot of attention unless there is a problem, and when there is a problem information security can quickly become a lightning rod for management's wrath. They need to be able to take the heat when there is a breach. Information security is also a highly politicized department, individuals need to be prepared for many political battles and to be able to get down and dirty when necessary. Similarly, the information security professional should be able to sell ideas and have excellent negotiation skills. He or she should be able to reach a compromise, but also be prepared to fight a battle and win it. The information security professional needs to be prepared to take unpopular stands and be able to stick with those stands when the going gets tough. The information security professional needs to exhibit leadership, be visible, and more and more he or she needs to be able to build a coalition. The information security professional also needs to be able to deal with a certain amount of ambiguity as in today's complex environments – many information security related decisions are not binary.

For someone considering an information security position, what signs can he/she look for to determine if the company is truly serious about information security?

If possible, it certainly helps to be able to interview the top management team (i.e. the CIO) to determine their own view of the importance of information security to the organization. Are they serious about information security and are they looking for someone to come in and be proactive as well as to facilitate difficult decisions, or, are they looking for a whitewash administrator or a place-holder manager.

You have commented before that a strong audit function can be important to the success of an information security function? How can internal audit and information security operate in a symbiotic manner?

I am very bullish on the long-term prospects of internal audit and information security working together, but it is important that they be separate functions. Audit can be a valuable conduit as they already have a trusted path directly to senior management. Audit can be an important independent voice to "wake up" management when they are ignoring information security. Audit can test and review the efficiency and effectiveness of the controls established and implemented by information security. In that sense they can act as a quality assurance function, a second set of eyes. This becomes more important as the complexity of business and information security increases. Audit can also be proponent of a well-staffed information security function. I have a free survey of information security staffing levels that I prepared with the Computer Security Institute; the survey allows readers to calculate the number of information security people they should have based on current staffing levels found in the same industry. To get a copy of the paper, anyone can call my office at 415/332-7763.

With the proliferation of client/server, and now e-commerce, the litany of technologies to keep up with and the sheer magnitude of potential security weaknesses seem overwhelming, don't they? This is challenging enough for companies with large information security groups, but how can the one or two person information security department possibly keep up?

A small department cannot afford to have technical specialists on any given technology – its not realistic or practical. More important, in these settings, is that they understand the processes and fundamental concepts of sound information security. They can also increase their effectiveness by subscribing to industry best practices. One way that companies can compensate for a lack of technical expertise on particular platforms is to bring in outside consultants or use an outsourcing firm. We are seeing an increasing number of information security functions like access control administration being outsourced.

Some companies have experimented with concepts such as "single-sign-on," for example, to try and grapple with this challenge, but with only limited success? Do you see any technical innovations on the horizon to enable a company to better secure their diverse platforms and connectivity without compromising functionality?

Yes. Digital certificates will absolutely revolutionize multi-platform and multi-organizational security. You will be able to sign forms with proof and authentication, enter into contracts over the Internet, determine access privileges or available credit. More and more organizations will incorporate this information into a process.

What kind of time frame do you foresee for this to hit mainstream use?

I would say two to three years, but it is coming on really fast. We are still working hard to create the infrastructure for PKI. There are reasons to believe that the current model of how to do this is not scaleable, so I believe it will have to change. There are also reasons to believe that we haven't adequately allocated liability for problems, and this too will force our current thinking and system design models to change. Also there are legal issues regarding jurisdiction to be sorted-through before certificates are ready for wide-spread use.

CALENDAR OF UPCOMING EVENTS

Date	Event	Place	Reference
March 21-27, 2000	SANS 2000	Orlando, Florida	www.sans.org
March 26-29, 2000	Euro CACS 2000	Oslo, Norway	www.isaca.org
May 7-11, 2000	North America CACS Conference 2000	Dallas, Texas	www.isaca.org
July 16-19, 2000	International Conference 2000	Lake Buena Vista, Florida	www.isaca.org
August 21-23, 2000	Network Security Conference	Las Vegas, Nevada	www.isaca.org
October 16-18, 2000	Latin America CACS 2000	San Jose, Costa Rica	www.isaca.org
December 4-6, 2000	eBusiness Conference	Las Vegas, Nevada	www.isaca.org

CISA COORDINATION

Justin Gibson
Committee Chairperson

The International Chapter of ISACA administers registration for the CISA exam (the next exam is scheduled for Saturday, June 10, 2000 – contact ISACA International to obtain registration materials). Please note that all registration materials for the exam must be completed by April 3, 2000. The cost for the examination is $325 for ISACA members and $425 for non-members. A discount of $30 will be given for registrations received before February 18, 2000. For detailed information regarding the CISA exam, please access ISACA International's Web site at: http://www.isaca.org/examinfo.htm.

The San Francisco Chapter is offering a complete review course for the 2000 CISA examination. This review course is designed to assist candidates in preparing for the CISA examination. The review sessions will be taught by professional IS audit, control and security professionals and will include lectures, classroom discussion, practice questions and exams. We have added one additional class this year to cover exam techniques and other items not specifically covered during the course. This will enable the instructors to focus on each specific domain during the review sessions. The four-hour review course sessions will be held on six Saturday mornings in downtown San Francisco beginning in April 2000. For more information on the course, please access the Chapter's Web site at: www.sfisaca.org/cisa.

The CISA Coordination Committee is responsible for developing and coordinating the Chapter's annual CISA Review Course. The committee also coordinates the annual CISA luncheon established to honor Chapter members who pass the CISA Examination. If you are interested in being part of the committee, please send me an e-mail: justin.gibson@us.pwcglobal.com.

In order to continue to offer an examination that measures a candidate's knowledge of current audit, security and control practices, new questions are regularly required for the CISA Examination. Questions are sought from experienced practitioners who can develop items that relate to the application of sound audit principles and practices. Continuing education hours and cash payments are offered as incentive to question writers. If you are interested in participating in the CISA Item Writing Program, please request information about the program from ISACA International, Certification Department (certification@isaca.org).

ACADEMIC RELATIONS

Eleanor Lee
Committee Chairperson

The Academic Relations Committee has been working hard to support the San Francisco State University (SFSU) IT Audit Curriculum and to take the program to the next level. The committee has identified a few companies that are willing to accept internships to provide opportunities for IT Audit students to gain valuable work experience. I would like to thank Todd Weinman and George Stool for helping in our efforts. Currently, Professor Eng, Business Analysis and Computing Department Chair at SFSU, is working with Wells Fargo and Kaiser Permanente to place two IT Audit students into the internship programs.

ISACA-SF board members, Kathleen Arnold and I attended the SFSU Accounting Students Organization Fall 1999 Awards Banquet on November 19, 1999 to award a scholarship that provides free admission to the ISACA-San Francisco Chapter's CISA Review Course and all the educational events for one year. Kathleen Arnold presented the scholarship to Richard Machado for the excellent work he has done in establishing SF-ISACA Student Chapter as a recognized organization. Due to Richard's efforts, the student chapter will qualify to receive funding from SFSU in Spring 2000. The funding will help the chapter build a stronger chapter by developing SF-ISACA Chapter members' technical knowledge and skills through technical presentations and workshops and promoting the IT Audit profession through new brochures, a Web site, and other communication channels.

In addition, the committee continues to make great progress with the Golden Gate University (GGU) IT Audit Curriculum project. We are in discussions with GGU Accounting Department Chair, Jim Schwartz, to discuss the implementation of an IT Audit Curriculum at GGU. The committee is developing an IT Audit Curriculum program by reviewing the GGU accounting and information technology courses and mapping them to the courses recommended by the IT auditing profession.

I would like to thank the Academic Relations Committee members for devoting their time and efforts on various projects. There is a great deal of work that remains to be completed and if you are interested in helping out with our exciting and rewarding efforts, please contact me.

Please contact me if you are interested in helping out with these important and rewarding initiatives.

Richard Machado
Outgoing Student Chapter President, SFSU

The Fall semester was an outstanding one for the student chapter at San Francisco State University. With the help of the San Francisco Chapter we have reached all of the goals that we set out to accomplish this semester. We would like to give special thanks to the following ISACA members: David Fong, Edmund Lam, Carol Hopkins, Kathleen Arnold, Lance Turcato, Karina Daza, and Eleanor Lee for all their support and direction.

Our accomplishments for the Fall were:

- Revamped the SFSU IT Audit Curriculum Brochure
- Designed a brand new ISACA Brochure for university chapters
- In the process of designing and implementing a SFSU chapter Web site
- Doubled the student chapter membership
- In the process of writing Policies and Procedures for the SFSU student chapter, so that the future presidents will have a foundation upon which to build

As I leave my position as President, I am proud that we have set-up the ISACA student chapter with all the tools needed to become an IT leader on campus for the semesters to come. I would like to give special thanks to all of the student chapter officers and members for all their hard work and I know that the new incoming President, Jonathon Suryadi, will continue the legacy.

Jonathon Suryadi
Incoming Student Chapter President, SFSU

Thanks to a great push that Richard Machado has provided, the ISACA SFSU student chapter is growing stronger. Having built a strong foundation, we look forward to exploring the uncharted territory, and it will certainly be challenging. However, knowing that we have the support of Dr. Jamie Eng, Dr. Kenneth Leong, our faculty advisors, and the ISACA board members, there is no doubt in my mind that we will, not only perpetuate the chapter, but make the chapter to be a highly recognized organization on campus.

Our goals for the upcoming semester:

- Increase membership – Our main goal for this semester is to increase our membership.
- Increase awareness on campus of ISACA and the IT Auditing curriculum – The general business students are not aware of this new major and an organization that supports it. Our target is to get ISACA linked with the IT Audit curriculum so that students cannot possibly think of majoring in IT Audit without joining ISACA.
- Finish the student chapter's Web site – With our account set up, we are now ready to design the Web page. This certainly will be fun and a good education for us!
- Work closely with the ISACA board members – A chance for us to work closely with the professionals! No doubt that this will help us transform from being students to becoming professionals.

In closing, I would to express gratitude to all of ISACA board members. Especially: Carol Hopkins, the ISACA president, for allowing us to observe the board meeting, Edmund Lam for expecting and demanding no less then 110 percent of energy in everything that we do, Eleanor Lee, for her support, Karina Daza, for her wisdom, and most certainly, the man who started the organization on campus, my friend, Sumit Kalra. By the way, for those of you who are wondering, yes, we are Year 2000 ready!

Transitioning Out of Audit

by Sandy Geffner

Sandy Geffner is a former IS Audit Director and Manager who is currently President of Valacon, Inc., a professional search firm specializing in IS Audit. He has passed the CISA and CPA examinations, and his article, "Introduction to Auditing Microcomputers", was published by Auerbach. Sandy is very active in ISACA, serving on the Board of the Los Angeles Chapter and Co-Chair of the 1995 International Conference.

Many auditors enjoy auditing and want to stay in the profession for a long time. This is great – they are doing something they enjoy. Others enjoy auditing but plan to transition into other areas. (Of course, some don't enjoy auditing, and they try to transition as quickly as they can.)

In strong economic times like we are currently experiencing, auditors are in strong demand, and there frequently will be opportunities for you to move into another area within your current company. This is the easiest transition because you know the company, and they know you. You have had a chance to develop contacts and establish a reputation. This enables you to win positions over other applicants who may have stronger specific experience than you do.

However, your current company may not offer the kind of position you would like, or your path may be blocked. In that case, your next move is usually to another company. That move can be to another audit department, or directly to a new area.

Moving directly to a non-audit position may sometimes be a little more difficult than you anticipate. Since the new company does not know you well, they may not offer you a position, or they may undervalue your experience and offer a position that is a step back. This can be a case of one step back for two steps forward which is okay, but it also could be a limiting move instead.

Another option is to transition to the new company in audit. If it is a company where you see a potentially strong future for yourself, and they have an established track record of auditors moving into the company, it may well be worthwhile for you to stay in audit a little longer in exchange for better long-term opportunities. Your odds of obtaining an offer are greater because you are capitalizing on your current experience. There are also secondary advantages to this approach. An audit position may enable you to gain a better, overall company perspective than going into a specific department. In addition, it's always a risk going into a new company, and audit is an excellent place for you to get a good feel for which department(s) would be best for you before you commit to one. You can then make a better career decision when you transition out.

EDUCATIONAL OFFERINGS

Todd Weinman
Committee Chairperson

January 18, 2000

Career Perspectives

Luncheon Presentation (high-level discussion)
11:30 AM – 2:00 PM

Afternoon Session (detailed presentation)
2:00 PM – 4:00 PM

February 15, 2000

IS Audit Best Practices – Session I

Luncheon Presentation (high-level discussion)
11:30 AM – 2:00 PM

Afternoon Session (detailed presentation)
2:00 PM – 4:00 PM

March 21, 2000

Secure Network Communications

Luncheon Presentation (high-level discussion)
11:30 AM – 2:00 PM

Afternoon Session (detailed presentation)
2:00 PM – 4:00 PM

Changes in 2000

In an effort to better meet the needs of our members, we are implementing a number of changes for the coming year. Starting in January 2000, we will be going to a somewhat different format for our monthly seminars. Instead of two distinct seminars (a one hour lunch presentation and a four hour afternoon seminar) we will be concentrating on one topic for the day. Typically, this will consist of a higher level luncheon presentation followed by two or more hours of more technically detailed material in the afternoon (timing will vary depending on the topic and presenter).

This year we will also feature two IS audit Best Practices seminars followed by panel discussions. Rather than focusing on particular technologies, these sessions will allow the membership a more interactive forum to explore successes and challenges faced by their fellow IS auditors in a variety of areas.

In addition to our monthly seminars, we plan to hold a number of special one or two day seminars in which we can get into a greater level of detail than in the monthly sessions. We also plan to hold a mini-conference later this year. You will find more information on the Web site and future newsletters and bulletins as details unfold.

ANNOUNCEMENTS

Refer A New Member – Receive A Free Gift

Take advantage of the Chapter's *New Member Referral Program*. Chapter members who refer an individual who joins ISACA – San Francisco Chapter will receive a free gift (gift will be delivered to the referring member after payment for the new membership has been received and processed by ISACA International). Don't miss an opportunity to help your colleagues keep abreast of developments in IS audit, security and control. Encourage your colleagues and friends to join ISACA today! For more information or to submit your referral to the *New Member Referral Program*, please send our Membership Committee Chairperson, Hector Massa (hlmsa@aol.com), the name, address, phone number, and email address for the individual being referred.

ISACA International

(847) 253-1545 voice • (847) 253-1443 fax • www.isaca.org

membership@isaca.org • certification@isaca.org
education@isaca.org • bookstore@isaca.org
conference@isaca.org • research@isaca.org
marketing@isaca.org

Y2K Contingency Planning Listserv

The purpose of this listserv is to enable individuals to provide information, ask questions, and share knowledge on this timely topic. While there are many general listservs, many dedicated to Y2K, this list is unique because it addresses Y2K contingency planning specific to IS professionals. To join the listserv, e-mail y2k-contingency-request@share.isaca.org. In the body of the message, type SUBSCRIBE. This listserv is sponsored by ISACA™.

Your E-mail address

If you have not sent your current E-mail address to ISACA International, then please send your address to hlmsa@aol.com to ensure that you receive important information electronically.

You may also access our Web site at www.sfisaca.org to update your contact information.

SPONSORSHIP COORDINATION

Edmund Lam
Committee Chairperson

It was a busy quarter for the Sponsorship Coordination Committee. I am honored to report to the members that ISACA-San Francisco has received quarterly sponsorships from Valacon and KPMG for the first and third quarters of 2000. On behalf of our organization, I would like to thank Valacon and KPMG for their support of our Chapter. As with past sponsorship funds received, we will commit the resources towards organizational excellence. This will include the continuous support of our educational programs and funding towards the award-winning Newsletter.

The Sponsorship Coordination Committee is also working diligently with at least two additional organizations to confirm sponsorships for the second and fourth quarters in 2000. If you would like to know how your organization can participate in this important program, please contact Edmund Lam at 510/987-0483 or at edmund.lam@ucop.edu.

An overview of the benefits our sponsors gain from participation in the Chapter's sponsorship progra is included below.

Sponsorship Benefits

Item	Benefit Derived
Monthly Bulletin	Sponsors are recognized in three monthly bulletins (all three months in the applicable quarter).
Quarterly Newsletter	Full-page ad allocated for the Sponsor. The Sponsor is provided with the opportunity to include an ad of their choice (i.e., recruitment opportunities, market services, etc.)
SF ISACA Web site	Sponsors are highlighted on the Chapter's Web site (www.sfisaca.org). We include a link to each sponsor's Web site and provide the sponsor with the opportunity to include an ad on the Chapter's Web site.
Monthly Luncheon	Sponsors are announced at each monthly meeting during the sponsored quarter. Sponsors are provided with the opportunity to provide materials (e.g., marketing, recruiting) for distribution to the meeting attendees.
Monthly Seminars	Sponsors are announced at each monthly seminar during the sponsored quarter. Sponsors are provided with the opportunity to provide materials (e.g., marketing, recruiting) for distribution to the seminar attendees.
Annual Recognition and Member Appreciation Luncheon	Sponsors are honored at this annual event. Sponsors are provided with the opportunity to provide materials (e.g., marketing, recruiting) for distribution to the attendees.

VALACON, INC.

Professional Search & Placement Specialists

"We Practice Quality"

Sandy Geffner: 11 years experience as an IS Audit Director/Manager including Big 5 Consulting experience; passed the CPA and CISA exams; B.S. in Math and MBA; active board member of ISACA-LA and 1995 International Conference Co-Chair; speaker for ISACA, IIA, AITP and ISSA.

Stuart Fried: Over 17 years in search and placement; prior experience as internal auditor and corporate accountant; taught university accounting; B.S. in Accounting and Marketing and M.A. in Clinical Psychology; Membership Co-Chair of ISACA-LAand 1995 International Conference Co-Chair.

Sarah Bulaon: IT recruiting; 10 years experience with Disney, Telecheck, Citibank Mortgage and The Warren Group in human resources and corporate administration.

Helen Kang: Audit and Financial recruiting; CPA; experience with Arthur Andersen, LLP and Mark Dauberman CPA Review Course; B.S. in Accounting and Communications; active board member of IIA-SFV.

Valacon, Inc. ***is a professional search and placement firm specializing in:***

- **Information Systems Audit**
- **Information Technology**
- **Financial/Operational Audit and Finance/Accounting**

Our approach is to properly assess and match our candidates with our clients. Unlike other firms who are sales and deal-oriented, we focus on developing and maintaining long-term, honest and ethical relationships with our clients. Each member of the Valacon team has valuable business experience; we truly understand our clients' needs and opportunities and correspondingly evaluate the skills and interests of our candidates.

Please see the **Candidate and Company Bill of Rights** on our website: **www.valacon.com**

PARTIAL LIST OF OPPORTUNITIES

- IS Audit Manager with High-tech co., start-up opportunity, ERP, E-Commerce, outsourcing and consulting. $100-$120K + Bonus + Stock Options
- IS Audit Director & Manager with Financial Services/E-Commerce co., technical, consulting, E-Commerce, $75k-$120s + Bonus
- IS Audit Manager & Senior with High-tech/Internet company, $70k-$100k + Bonus
- IS Audit Director with Specialty Retail co., manage consulting, sys dev and outsourcing. $100-$120k+ + Bonus + Stock Options
- Senior IS Auditor with Financial Services co., focus on business process and sys dev. $70s-80s + Bonus
- Senior IS Auditor with International Service co., technical, networks, sys dev. $60-$70k
- Senior/Staff IS Auditor with Financial Services co., UNIX/client server, sys dev. $60-$80k + Bonus
- Senior IS Auditor with Consumer Products co., special projects, int'l travel. $60s-$70s + Bonus
- Big 5 firms seeking Senior Managers, Managers, Seniors, Staff throughout California and the U.S.
- Opportunities in Southern California, Arizona, the Northwest, and elsewhere.

Please visit our website - www.valacon.com - for more information about these and other opportunities.

VALACON, INC. 466 E. Foothill Blvd., Suite 206, La Cañada, California 91011

Phone: (818) 949-7911 **Sandy:** (818) 949-7912 **Stuart:** (818) 949-7914
Fax: (818) 949-7916 **Sarah:** (818) 949-7919 **Helen:** (818) 949-7917
Email: **info@valacon.com** *Website:* **www.valacon.com**

SAN FRANCISCO CHAPTER BOARD ROSTER 1999/2000

Executive Board

President
Carol Hopkins
Providian Financial
415-278-4724
carol_hopkins@providian.com

1st Vice President
Edmund Lam
UC Office Of The President
510-987-0483
edmund.lam@ucop.edu

2nd Vice President
Todd Weinman
Lander International
510-835-3053
tweinman@landerint.com

Secretary
Karina Daza
Ernst & Young LLP
415-951-3060
karina.daza@ey.com

Treasurer
Bill Davidson
Bay Area Rapid Transit District
510-464-6954
wdavids@bart.dst.ca.us

Director/Past President
Lance Turcato
Charles Schwab & Co., Inc.
415-636-8158
lance.turcato@schwab.com

Directors

Directors
Kathleen Arnold
PricewaterhouseCoopers
415-291-6722
kathleen.arnold@us.pwcglobal.com

Hector Massa
Office of Thrift Supervision
415-616-1875
hlmsa@aol.com

Justin Gibson
PricewaterhouseCoopers LLP
415-547-3919
justin.gibson@us.pwcglobal.com

Sumit Kalra
Deloitte & Touche LLP
415-836-5413
skalra@dttus.com

Marcus Jung
Pacific Stock Exchange
415-393-7933
marcauditor@juno.com

Leah McKern
PricewaterhouseCoopers
415-369-1243
leah.j.mckern@us.pwcglobal.com

Eleanor Lee
Providian Financial
415-278-4653
eleanor_lee@providian.com

Committees

Academic Relations
Eleanor Lee, Chair
David Fong
Karina Daza
William Luk

CISA Coordination
Justin Gibson, Chair
Sumit Kalra
Helen Leung

Communications
Lance Turcato, Chair
Christina Cheng
Swee Fuller
Carol Hopkins
Sumit Kalra
Allison Leeds
Esther Silver

Education
Todd Weinman, Chair
Kathleen Arnold
Deborah Frazer
Marcus Jung
Eleanor Lee

Membership
Hector Massa, Chair

Sponsorship
Edmund Lam, Chair

Web Master
Lance Turcato, Chair

Advisory Board

Advisory Board
Robert Abbott
Blair Bautista
Arnold Dito
Kathryn Dodds
Charles Dormann
Douglas Feil
Roberta Hunter
William Luk
Susan Snell
Richard Tuck

ISACA – San Francisco Chapter
Communications Committee
PO Box 26675
San Francisco, CA 94126

Newsletter design by ALLISON M. LEEDS GRAPHIC DESIGN 415 522 0788