SAN FRANCISCO CHAPTER | LOCAL AREA NETWORK

THIRD QUARTER 2007

ISACA
Serving IT Governance Professionals
San Francisco Chapter

PRESIDENT'S MESSAGE

Mike Nelson, CISA, CISM, CISSP, CAP, ITIL, PRESIDENT

A FINAL NOTE: CHAPTER REMAINS HEALTHY AND STRONG

As my term as chapter President comes to a close and the torch is passed to a new leadership team, it seems altogether appropriate to reflect on the past year in terms of what we've accomplished and the challenges that remain ahead of us. I was extremely fortunate to have a strong and active Executive Committee and team of Directors, Committee Chairs and Volunteers. As many of you have heard me say in the past, we each have control of our own character, but others own our reputation. The leaders of the San Francisco Chapter are in many ways demonstrating their character and building their reputation within our professional community.

When I was elected to the role of President, I set some personal goals for myself to make a mark on the chapter and leave it in a condition at least as healthy as the one I inherited from Mike Villegas. My number-one priority was to not break anything. We have a long history of providing value to our members and I saw it as a primary goal that we continue that performance trend. I'm proud to report that we have maintained that legacy.

Our chapter is financially strong, our membership numbers continue to grow, our renewal rates are among the highest in ISACA and attendance at our chapter events continues to swell. Our Education Committee has made a real push to ensure the luncheon sessions, day-long technical sessions and joint sessions with sister organizations are relevant, timely and perceived as valuable. Our CISA and CISM workshop committees continue to attract full classrooms of exam candidates from a wide geography. We've had people from the US East Coast as well as Canada and Mexico fly into San Francisco to take advantage of our exam preparation workshops.

Our annual Fall Conference continues to grow and the 2007 conference is shaping up to be a great event. This year, we are the host chapter for the annual Western Region Presidents Council Meeting, so the leaders of the 24 Western Region (US and Canada) chapters, as well as representatives from ISACA International will congregate in our City for a weekend of intense discussion on chapter operational best practices.

Our volunteers continue to be the heart and soul of our chapter. Nothing would get done without the dedication and commitment of professionals from throughout our organization. There is such a wide variety of needs our chapter has for volunteers that virtually anyone can find some way to contribute that fits into their availability and skill set. Some important opportunities will arise in the upcoming year as we work to take a fresh look at our event registration and payment requirements and options, as we try to step up to even greater involvement with ISACA International activities, including research, exam item writing and CobiTO development and deployment support and as we support the emerging ISACA Certificate in IT Governance.

As I move into the Past President role for the next year, I plan to provide the support and guidance that the incoming leadership team will benefit from and I hope that each of you will work to find the time and energy to give back to your profession. I know from experience that doing so can be both rewarding and fun.

CONTENTS

The San Francisco Chapter of ISACA proudly presents...

SF ISACA 2007 Fall Conference

IT Audit

Information Security

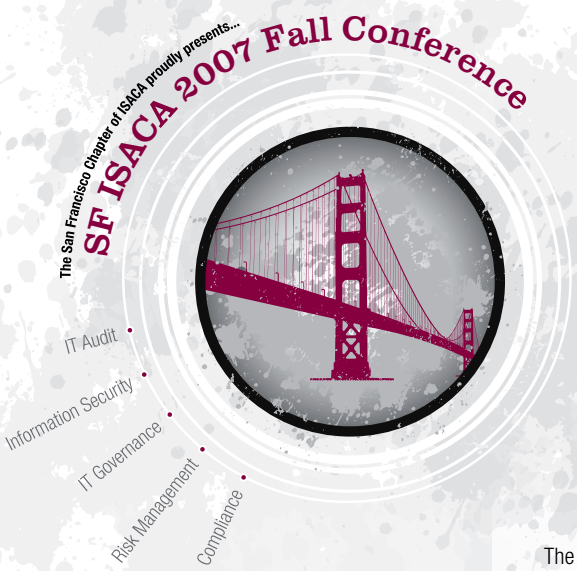
IT Governance

Risk Management

Compliance

BRIDGING THE GAP

September 17–19, 2007



BRIDGING THE GAP

September 17–19, 2007

The SF ISACA Fall Conference is the premier education event for Information Systems Audit and Information Security professionals in the Northern California area. Last year's event drew nearly 200 IS Audit and Security professionals and we are expecting higher levels of attendance this year.

Priced at $500 (member early-registration rate), roughly 1/3 what many similar conferences charge, the SF ISACA Fall Conference represents Northern California's best educational value for IS Audit and Security professionals.

The 2007 SF ISACA Fall Conference features four tracks:

The Core Competencies track focuses on the fundamentals of IS audit. It is ideal for IS auditors in the early part of their career, those transitioning into IS audit, as well as more experienced IS auditors that may be interested reviewing or in developing a new skills set. This track is also of value to Chief Audit Executives and Internal Audit Directors and Managers who manage the IS audit function or IS auditors.

The Information Security track features sessions on the most current security topics to enhance the skills of IS audit and security professionals. It is ideal for those individuals who want to make the connection between protections of Information Confidentiality, Integrity and Availability and the audit evidence necessary to demonstrate control effectiveness. Those considering the Certified Information Security Manager (CISM) certification will benefit from the topics covered in this track.

The IT Governance track covers a variety of topics of relevance to IS auditors, as well as IT and Compliance professionals. These sessions will address new techniques, methodologies and practices pertaining to IT Governance, as well as exploring the value of effective IT Governance.

The In-Depth Technical track will offer three full-day sessions on key topics of high interest to our membership: Infrastructure Vulnerabilities, Windows Vista Security, and Hacking 101: Understanding the Top Web Application Vulnerabilities and How to Protect Against the Next Level of Attack.

In addition to the educational sessions, the 2007 SF ISACA Fall Conference will also feature an **Exhibitors Hall** and **Exhibitors Lunch** on Tuesday, September 18th.

This will allow attendees to visit with vendors serving the industry. Look for updates on our web site at: **www.sfisaca.org**. The registration and payment capabilities will be enabled circa July. **Make your plans to attend today!**

About the Keynote Speaker:

Rena Mears

Partner, Security Services

Rena is the Global and National Service Line Leader of the Deloitte Privacy Team and West Coast leader for Deloitte's Security Services practice. She is an internationally recognized expert in security and privacy. Rena has more than 20 years of experience in security strategy and program design, enterprise security architecture (ESA), and secure infrastructure implementation. She has authored articles on wireless technology, customer and employee privacy and security in the enterprise. Rena is a key advisor to several organizations including the International Association of Privacy Professionals, the American Bar Association, and the AICPA's Assurance Services Executive Committee. Rena has a B.A. from the University of Albuquerque, and a MBA from Auburn University.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Conference Schedule

Monday, September 17, 2007	Core Competencies	Information Security	IT Governance	In-Depth Technical
7:15 am to 8:45 am	Registration and Breakfast			
8:45 am to 10:00 am	Welcome and Keynote: Rena Mears			
10:00 am to 10:15 am	Networking Break			
10:15 am to 11:45 am	Session C11 Intro to IT Auditing for Non-IT-Auditors Steve Shofner	Session S11 Web Application Security: Finding Vulnerabilities in Dynamic Applications Mike Shema	Session G11 Project Risk Management Brett Curran / Sheryl "Kahki" Perrine	Session T1 Windows Vista Security Don Hester
11:45 am to 1:15 pm	Luncheon Speaker: Daniel Morrison - PwC			
1:15 pm to 2:45 pm	Session C12 COBIT Fundamentals and Uses Mike Villegas	Session S12 Information Leak Prevention: How to Tame the Insider Threat Aaron Weller	Session G12 COBIT / VALIT Kendall Tiek	Session T1 Windows Vista Security (Continued) Don Hester
2:45 pm to 3:00 pm	Networking Break			
3:00 pm to 4:30 pm	Session C13 Beyond SOX: Adopting ITIL Chad Kalmes / Paulina Fraser	Session S13 Continuous Monitoring (HP & Google's Perspective) Jessica Amezquita / Brad Ames / Erik Jonte	Session G13 Security Effectiveness Metrics: Creating a Compelling Business Case Yong-Gon Chon	Session T1 Windows Vista Security (Continued) Don Hester

Tuesday, September 18, 2007	Core Competencies	Information Security	IT Governance	In-Depth Technical
8:30 am to 10:00 am	Session C21 Intro to User Access Controls Tony Goulding	Session S21 How to Protect from Malicious Code: Using Honeynet and Darknet Technology as Part of a Compliance Program Michael Smith	Session G21 Leveraging IT Audit Resources: IT Risk Assessment Trough High-Impact Audits Jerry Meyers	Session T2 Infrastructure Vulnerabilities Derek Koopowitz
10:00 am to 10:15 am	Networking Break			
10:15 am to 11:45 am	Session C22 Intro to Change Management Controls Biriam Debrezion	Session S22 Security Effectiveness: A System Settings Perspective Rodney Kocot	Session G22 Enterprise Risk Management Gary Ross	Session T2 Infrastructure Vulnerabilities (Continued) Derek Koopowitz
11:45 am to 2:15 pm	Exhibition Fair & Luncheon			
2:15 pm to 3:45 pm	Session C23 Intro to IT Operations Controls Sandee Lim / Kalpa Chobe	Session S23 Wireless Systems Vulnerabilities, Threats, and Auditing Jeffrey Camiel / Rob Tillman	Session G23 Beyond SOX: High Value Audit Stephan Spalding	Session T2 Infrastructure Vulnerabilities (Continued) Derek Koopowitz
3:45 pm to 4:00 pm	Networking Break			
4:00 pm to 5:30 pm	Session C24 Intro to Application Controls Matt Hatch / Oliver Petri	Session S24 Endpoint Security Mark Kadich	Session G24 PMO Auditing Shawn Kirshner	Session T2 Infrastructure Vulnerabilities (Continued) Derek Koopowitz

Wednesday, September 19, 2007	Core Competencies	Information Security	IT Governance	In-Depth Technical
8:30 am to 10:00 am	Session C31 Intro to Database Auditing Scott Hayes	Session S31 Locating Sensitive Data in Structured Data Sets Ravi Jagannathan	Session G31 Control Rationization / Optimization David Willoughby	Session T3 Hacking 101: Understanding the Top Web Application Vulnerabilities and How to Protect Against the Next Level of Attack Armando Bioc
10:00 am to 10:15 am	Networking Break			
10:15 am to 11:45 am	Session C32 Intro to ERP Auditing Vanessa Balough	Session S32 Data Privacy - Protection From Trusted Users Doug Sanders / Scott Smith	Session G32 Operationalizing Security and Compliance: Generating Maximum Compliance ROI Mark Seward	Session T3 Hacking 101: Understanding the Top Web Application Vulnerabilities... (continued) Armando Bioc
11:45 am to 1:30 pm	Luncheon Speaker: Todd Weinman - Lander International			
1:30 pm to 3:00 pm	Session C33 Intro to Computer Assisted Auditing Tools (CAATs) Carl Bledsoe / Rudy Chavez	Session S33 Leveraging FISMA Guidance to Support an Effective Risk Management Strategy To Secure IT Systems and Meet Regulatory Requirements Thomas Chimento / Bill Robinson	Session G33 End User Computing Terry Nystrom	Session T3 Hacking 101: Understanding the Top Web Application Vulnerabilities... (continued) Armando Bioc

The SF ISACA Chapter would like to thank the following organizations
for their support and contributions for the 2007 SF ISACA Fall Conference:

Platinum Sponsor

Deloitte.

Gold Sponsors

ArcSight

Ernst & Young
Quality In Everything We Do

KPMG

PricewaterhouseCoopers

protiviti®
Independent Risk Consulting

Robert Half® Management Resources
Project Financial Professionals

Silver Sponsors

EXEROS

Jefferson Wells
A Manpower Company

Lander International, LLC
Because Your Search is THAT Important

netIQ
An Attachmate® Business

Valacon, Inc.

VONTU

PROCTORS NEEDED FOR FALL CONFERENCE SESSIONS

The seventh annual San Francisco ISACA Fall Conference is fast approaching. This three-day conference, from September 17- 9, will have more than 30 sessions in four tracks covering Core Competencies, Information Security, IT Governance and In-Depth Technical topics. The Education and Conference Committees have done a wonderful job in getting top-notch presenters for these sessions.

However, one detail remains.

The Conference Committee needs your help as a session proctor. The main responsibility of the proctor is to be the ISACA support person at the assigned session. The proctor assists the presenter with any special needs (most set-ups are arranged in advance). The proctor also introduces the presenter by reading from a prepared bio. The proctor also distributes and collects the session evaluations.

Support the Conference by being a session proctor. To volunteer or ask questions, please contact Tim Stapleton at 415-243-5937, or at tim.stapleton@wellsfargo.com.

THE IT AUDIT PROFESSION – JACK OF ALL TRADES

By Miguel (Mike) O. Villegas, CISA, CISSP

If you take 20 CEO's of any Fortune 1000 company, place them in a room and ask them what the primary goal of their business is, they would say it's to maximize shareholder wealth. It is not to be the best company in their industry, the most technologically advanced or the preeminent center of excellence in controls and security. These and many more are obvious byproducts of the primary goal. If the enterprise is not gaining wealth, other ancillary goals are of lesser consequence. Executive management has always known this. However, management may pursue this profit-maximizing objective provided they maintain the privacy, security, integrity and availability of information.

Having been involved in the IT audit and information security professions since 1978 working for large banking and what was then Big 5 accounting firms, I have seen many institutions that run the IT control spectrum of great, to good, to very bad. Information security evolved from a central mainframe environment with dumb terminals connected via communications controllers to a ubiquitous open system architecture where every system has connectivity to every other system even without the proverbial hard wire.

Information security challenges have multiplied thousands of times since the days of MVS/370 and punch cards. Security professionals used to be concerned with only access controls over production data, access privileges of application and system programmers, security over computer operations, physical security of the data center and disaster recovery planning. Today, we have multi-operating system platforms, mobile computing, wireless technology and, of course, the Internet (including intranets and extranets) with virtual 24/7 connectivity to anything.

This is not news to anyone. But have IT auditors kept up?

IT auditors are perceived as jack of all trades but master of none. This is because we, as IT auditors, are required to look at all high risk IT environments, application and business processes and provide management assurance that commensurate controls are working effectively to manage (not eliminate) risk to an acceptable level. I have always contended that IT auditors, although jack of all trades, need to be master of at least one. Every auditor should find their niche and be its risk-and-control expert. This can be difficult in smaller institutions but necessary nonetheless.

How can the auditor find his/her niche? The obvious one is to delve in the area of greatest personal interest. However, the auditor needs to ensure that this technical area is in line with where technology is going or will exist for years to come. Read manuals, interview subject matter experts, take in-depth technical training in the area, perform technical audits and eventually share or teach others. Typically, in preparing for teaching on a particular topic, the instructor needs to have real-world experience as well as expert knowledge in the area.

IT audit professionals need a working knowledge in networking, Internet technologies, Web-based application security, security administration techniques, PKI, multiple platform environments with different system architectures and resource/id naming conventions. IT audit plans today include audits of the usual operating systems such as mainframe, mid-range and client/server environments (e.g., z/OS, Tandem, iSeries, UNIX and Windows Servers). However, they also include audits of vendor management, risk management, information security, web-based services, wireless technologies, biometrics, computer forensics, incident response, business continuity planning and key industry risk-based applications and processes. Who can keep up?
Information security has historically been considered a necessary evil and many companies have taken the approach that it take a back seat to other more important matters, such as uptime, response time and budgets. Even regulated industries have traditionally wanted to implement controls just enough to get a passing grade from regulatory agencies rather than focus on commensurate risk-based controls.

Having fought (and still fighting) many battles to strengthen security in many institutions, I now find a renewed interest in risk, compliance, security and privacy. Some of this could be due to the terrible incident of September 11 and Enron, but I believe that executive management is now realizing that in order to serve and protect the interests of their customers and shareholders, they must take on the challenge of ensuring much more the safety and security of

information systems. We have become so dependent on technology that without it today many institutions could easily falter within days of system outages or illegal system penetrations.

Personally, I do not believe IT auditors need to be an expert in all technologies. My "niche" is mainframe security, risk management and web-based application controls. IT auditors, however, definitely need to be experts in risk, control structures and compliance.

Someone said that aging is a hard price to pay for maturity, but it doesn't have to be that way. Don't take an NIH (not invented here) attitude about controls and security because believe me, they have not changed all that much. Technologies certainly have changed, but controls and information security are essentially the same.

We have seen improvements in risk management systems for IT, information security and IT audit that focus on key business IT environments. Frameworks such as COBIT, ITIL, NIST and standards such as ISO 17799 have allowed us to ensure we cover pertinent areas of risks and controls. These have especially been instrumental in guiding compliance activities for Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and Sarbanes-Oxley.

But the basics still exist. We are still dealing with CIA (confidentiality, integrity and availability), IAA (identification, authentication and authorization). We still need to implement deterrent, preventive, detective and corrective controls placed as close to the point of entry as possible. We must still address poorly configured baselines, change controls, separation of duties, access authorizations commensurate with job responsibilities, audit trails, management trails, security software, auditing, policies, procedures, security awareness, "ethical hacking" (if there is such a thing), security and privacy, regulatory requirements, security administration, BCP, monitoring, accountability, integrity and responsibility.

No matter how robust technology control features have evolved, they are for the most part installation selectable. These features are frankly just not turned on. As I have performed, managed and reviewed IT audits, information security reviews and risk assessments, I still find issues related to access control, baseline configuration, separation of duties, security vulnerabilities, documentation, change control, regulatory compliance and risk management.

For example, where in the past I would find supervisor-state programs (i.e., Authorized Program Facility – APF) uncontrolled that allowed circumvention of mainframe security constructs, I now find web applications that are subject to cross-site scripting vulnerabilities, buffer overflows, directory traversals or damaging SQL injections. The technology and control features have clearly improved, but the issues are still the same.

We are still dealing with the people factor. People still commit mistakes, inadvertent or intentional destruction of valuable information, fraud, theft, terrorism, unauthorized or excessive access, hacking or even just playing games at someone else's expense. That is just the nature of our profession.

Can you be a master of all technologies? Definitely not. Can you be a master of at least one? Certainly. But no matter what route you take, be a master of risk, security and controls. Stand up to the challenges that face you. Keep up with technology but more importantly, understand risk. Balance risks and controls based on strategic business objectives. Ensure that these controls are cost effective. Focus on your organization, your customers, your career, your ethics, and your business goals. Know when to ask for help, but develop and improve yourself. Find your niche. Have pride, passion, drive, integrity and a work ethic that does what is right and not just what is expected. Have fun. Hire employees who share your passion. Manage and lead by example. Don't be afraid to recommend controls or make mistakes, but by all means, don't be quixotic. Don't spend what you don't have, but spend what you need. Don't buy a name alone. Buy experience, objectivity, skills and knowledge. Be an ambassador for risk-based security and privacy. These are what make this such a grand profession. These are what make you great.

Disclaimer: The opinions expressed in this document are strictly the opinions of the author. It is intended to express observations on the challenges confronting the IT audit and information security profession as a whole. (August 2007)

INTEREST AND PARTICIPATION ARE HIGH IN CISA REVIEW AND EXAM

San Francisco CISA Review Course
More than 20 people took the CISA San Francisco Review Course this year. The review sessions were taught by IS audit, control, security, and business advisory professionals, and included lectures, classroom discussions, practice questions and exams. Thank you to the instructors who volunteered: David McKenzie from Wells Fargo, Stephen R Shofner from Williams-Sonoma, Vikram Panjwani from PricewaterhouseCoopers and Mike O. Villegas from Wells Fargo.

CISA Examination

Hundreds flocked to take the CISA exam on Saturday, June 9. Good Luck to those who have taken the exam this year! For those who missed the exam this year, the exam is administered bi-annually on the second week of June and December. For more information on the CISA exam, please access the San Francisco Chapter's ISACA Web site at: www.sfisaca.org/cisa.

Benefits of becoming a Certified Information Systems Auditor (CISA)
Since 1978, the CISA program, sponsored by ISACA, has been recognized as the one international standard of achievement among IS audit, governance, control and assurance professionals. Passing the examination opens many doors for individuals with various strengths. The accomplishment for some may signify a chance to make more money, for others a promotion or prestige, and for many of us, a sense of accomplishment for reaching a goal in our careers. Being recognized as a CISA brings with it a great number of professional and organizational benefits. Successful achievement demonstrates and attests to an individual's information systems audit expertise and indicates a desire to serve an organization with distinction. This expertise is extremely valuable given the changing nature of information technology and the need to employ certified professionals who are able to apply the most effective information systems audit, control and security practices, and who have an awareness of the unique requirements particular to information technology environments. Those who become CISAs join other recognized professionals worldwide who have earned this highly sought after professional designation. Although certification may not be mandatory for you at this time, a growing number of organizations are recommending that employees become certified. The CISA designation assures employers that their staff is able to apply state-of-the-art information systems audit, security and control practices and techniques and that these skills are maintained. For these reasons, many employers require the achievement of the CISA designation as a strong factor for employment and/or advanced promotion.

PricewaterhouseCoopers Sponsorship
As result of the generous sponsorship of PricewaterhouseCoopers this year, the San Francisco Chapter was able to maintain and not raise the fees for the CISA Review Course. Thank you PricewaterhouseCoopers!

ISACA Exam Identification Policy

Each candidate taking the CISA/CISM exam must submit and will only be admitted to the test center if they have a valid admission ticket and an acceptable form of identification (ID). An acceptable form of ID must be a current and original government issued identification that contains the candidate's name as it appears on the admission ticket, and the candidate's photograph. All of these characteristics must be demonstrated by this single piece of ID provided. Examples include, but are not limited to a passport, driver's license, military ID, state ID, Green Card and national ID. Any candidate who does not provide an acceptable form of identification will not be allowed to sit for the exam and will forfeit his/her registration fee.

If any specific questions or identification issues arise within your chapter, please feel free have the candidate or yourself contact the certification department at certification@isaca.org or 1.847.253.1545 Ext. 772. Again, thank you for your assistance.

Scenes from the CISM Exam Prep Workshop
Instructor Jason Kobus, right, guides students through the CISM Body of Knowledge. CISM students focus on preparing for the exam.

NEW LEADERS ANNOUNCED, PAST LEADERS HONORED AT CHAPTER AGM

Members and no-members attended the San Francisco Chapter All General Meeting on July 19 at Hotel Nikko in San Francisco to enjoy an evening of networking, cocktails and hors d'oeuvres. They also enjoyed a night when new chapter leadership was announced and past leadership was honored.

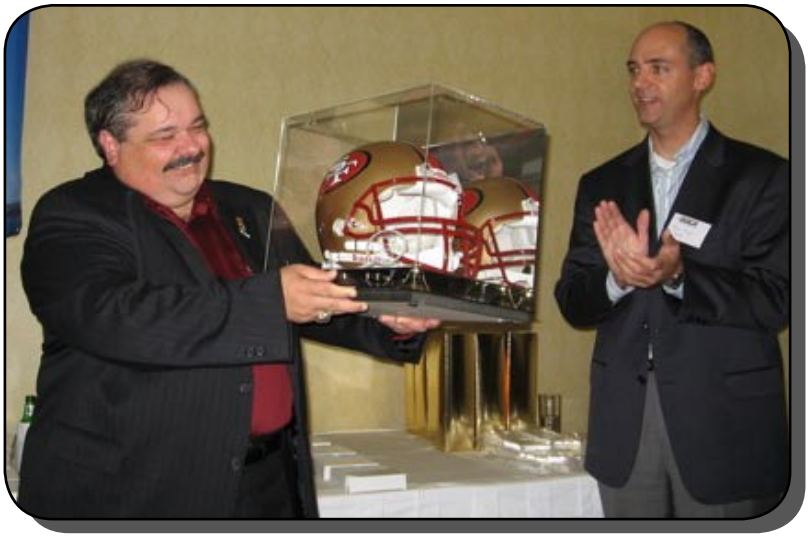
At the midpoint of the AGM, Chapter Election Committee member Debra Mallette made the announcement that Kevin Fried garnered the majority of the votes received, and was elected as the new chapter president. Like Fried, Conny Cheng and Tim Stapleton received majority vote in their elections to First and Second Vice President, respectively. Ashok Kumar and Sandy Lee were re-elected as the chapter Secretary and Treasurer, respectively.

Outgoing president Mike Nelson was honored for all the work hard he has given to the chapter when Fried presented Nelson, a devoted San Francisco 49ers fan, with a special gift – an authentic San Francisco 49ers football helmet.

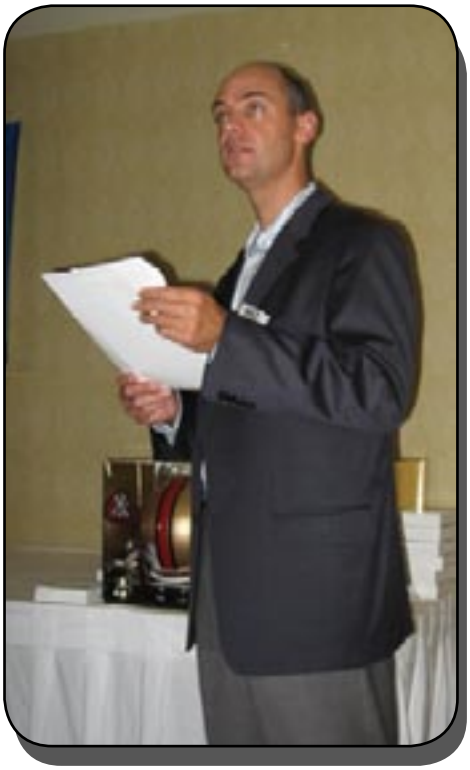
It was also announced that Todd Weinman, Christina Cheng and Vikram Panjwani were elected as chapter Directors, who serve two-year terms on the leadership board.

According to the Report of the Election Committee filed by Mallette and Bill Davidson, 44 total votes were cast during this election. The 44 votes represented 20 percent of the chapter membership.

Other chapter leaders and volunteers, and people who passed the CISA/CISM exams, were also recognized at the AGM.



Mike Nelson holds up an authentic San Francisco 49ers football helmet as Kevin Fried applauds for all the hard work Nelson has given to the chapter as president.



Newly elected president Kevin Fried speaks to the AGM audience.

Attendees enjoy the food spread at the AGM.

Sandy Lee, left, and Mary Lee help AGM attendees find their name tags.

AGM attendees listen intently on the messages delivered throughout the event.

Chapter says "Speak Up"

The San Francisco Chapter is starting a speaker group. And we want you.

We are so fortunate to have so much audit and security talent here in the Bay Area, and by talent, we mean you. Each of you has some knowledge that would be valuable to you colleagues and/or others in the organizations that we all work with (those that we audit). We need to share that knowledge with each other, so the SF Chapter is starting a Speakers Group to fill that need.

Our first speaking opportunities will be at the upcoming Fall Conference. However, speaking opportunities come up all the time, and we are planning to have several presentations and speakers ready to go when those opportunities come.

Surgeons have a motto: "See one, do one, teach one." That's the approach we're planning to take to build our speakers. Unless you're already a master presenter, we will partner up-and-comers with more polished presenters. This will provide you with the opportunity to gain a better understanding of the presentation topic and an opportunity to see someone else's presentation style and pick up tricks and tips to help build your own skills. It also helps both presenters by splitting the load, which is a presentation approach with a proven record of success.

Initial presentations will start with basic IT audit & security concepts. Then we will further grow the presentation library by building on those concepts. The end result: a full library of standard education presentations, polished and ready to go; and a stable of well-versed, seasoned speakers ready to deliver them and share the great knowledge of our local area.

We also open to other ideas, if you have a burning topic that just needs to be heard. Just let us know, and we can find someone to partner with and build presentations for those as well.

Regardless of your current presentation skill-level, we hope you will join this group. Past experience is not required. Everyone has some knowledge or expertise that others will find valuable. Please join us and share that knowledge to help your fellow ISACA members, our organizations, and the business community in general. If you're interested, please contact Mike Nelson at mnelson@securenet-technologies.com or 925-833-0286.

Education Committee Message

First and foremost, the 2006-2007 Education Committee members thank you for your support and feedback for a successful program this past year. Part of that success was because of the initial feedback provided on the topics of interest to you collected at this time last year. To improve this process further and to tap a wider audience, the education committee is planning to automate the survey process to collect your input on topics you would like to hear about in the next year. We have already received emails from several speakers who would like to talk to you, the SFISACA community, and the committee will align potential speakers with topics you want to hear about. We plan to use a mixture of local chapter members, alliance events (e.g., ISSA, IIA, IAPP, etc.), multi-speaker panels, vendor sessions (informational and non-sales oriented), technical sessions and a full-day, professionally lead training course. Look for the survey in your inbox in a few weeks and let us know what you want to hear about.