



PRESIDENT'S MESSAGE



**CONNIE CHENG,
CISA, CPA, CFE, CISSP
PRESIDENT**

CHAPTER ACTIVITIES BLOSSOM IN THE SPRING

Welcome to the Spring Edition of the "Local Area Network," San Francisco ISACA's local quarterly newsletter. While the spring of 2009 has been challenging and hopeful for our country, it is an extremely busy and encouraging time for ISACA International and the San Francisco chapter. Let's quickly look back and then look forward.

ISACA International

While almost all of our members know very well the benefits of the CISA certification, there is recently another reason to be proud of being a CISA or to attain a CISA. CISA has won SC Magazine's award for Best Certification Program this year. In addition to CISA, the finalists of this award included (ISC)2, Global Information Assurance Certification (GIAC), CISM and Symantec Certification Program. For more details, please refer to <http://www.scmagazineus.com/Best-professional-certification/article/130888/>.

The CGEIT certification also has important news this spring. It has now been earned by more than 3,000 professionals. The second CGEIT exam will be held on June 13 along with the CISA and CISM exams.

ISACA San Francisco

The local chapter also has exciting news. Our chapter website (www.sfisaca.org), which has been diligently maintained by webmaster Mike Nelson, our former president and current membership co-chair, has won a Bronze-level award for 2008. We are all very proud of the work Mike put forth in the design, content and management of our chapter web site to earn this recognition. A big "thanks" to Mike!

In addition to the web-site award, we had a number of very successful educational events the past couple of months. Unlike the traditional luncheon events in San Francisco, these events were presented in varied formats and locations, reflecting our efforts to respond to our members' requests through last year's membership survey. On April 1, we hosted an all-day session on "Protection of Consumer Information" in Walnut Creek, allowing easier access for many of our members who live and work in the East Bay. We maxed out our capacity of 80 attendants in that event. On the late afternoon of April 29, we had a joint event with ITSMF, featuring a Cloud Computing Discussion Panel. Networking sessions were included both before and after the panel discussion during this event, allowing our members to connect with other IT audit and security professionals. This was also our effort to support our members in a very difficult economic time.

Another important event that is underway is a CGEIT Review Course. This review course was solely developed by Bill Pankey of Tunitas Group and offered to our members at no charge. Bill is extremely enthusiastic about the CGEIT certification and very knowledgeable about the topics. We are grateful for his efforts and generosity in sharing his knowledge with fellow members.

The Student Best Paper Contest is also underway. The contest is intended to introduce the IT audit and security profession to college students and encourage them to explore the numerous career opportunities in this profession. Students were encouraged to submit a paper written by them on the topics of the profession or selected IT audit and

CONTENTS

President's Message	1-2
Education Message	3-4
Best Paper Contest 2009	5-7
Committee Message	8
Membership Message	8
CISA CISM Technical Article	9-11
Fall Conference Info	12
Board Roster	13

PRESIDENTS MESSAGE CONT'D.

security areas by May 8. Scholarships will be awarded to winners during the July annual general meeting. The winning paper will be published in future newsletters.

The board also has a new volunteer committee chair. Steven Majourau, a long time IT audit and security professional, has stepped into the Volunteer Committee Chair position, replacing former chair Kenny Cheng, who recently returned to the UK. Steven is also helping to lead the professional version of the Best Paper Contest. Welcome, Steven!

There are also many other activities that are currently in the planning mode and members should expect to see in the coming few months. These activities include

- The CISA review course that will take place on three consecutive Saturdays in May at the PwC office in San Francisco
- The Annual Membership Survey
- The Professional Version of Best Paper Contest
- Chapter Financial Policies, Procedures and Controls Development
- 2009/2010 Chapter Election
- Annual General Meeting in July
- May and June Monthly Educational Events
- Fall Conference Planning

I hope that all of you will take the opportunity to participate in these events and better yet, to volunteer your time by helping out the various committees. Should you have any suggestions, feedback, comments or questions, please don't hesitate to contact me at president@sfisaca.org. Looking forward to hearing from you!

Conny Cheng, CISA, CPA, CFE, CISSP
PRESIDENT

Education Message

By Thej Mehta and Heather Ouellette

Education Committee Co-Chairs

On the Education Front, the chapter has had a stellar calendar year to date, with record attendance and attendee feedback over previous years.

The April event, The Cloud Computing Panel, a joint event with the Local Interest Group of the Information Technology Services Mgmt Forum, (itSMF) with approximately 85 attendees, was an afternoon/evening event that was extremely well received. The event started with a 30-minute Networking and Hors d'oeuvres session, and was followed a 15-minute "primer" presentation, courtesy of one of the panelists. Over the next two and a half hours, the speakers were able to cover many aspects of Cloud Computing, including Service Management, executing a Cloud Computing model, and Security, Privacy and Compliance in the Cloud. The Q&A portion of the session allowed members to get their serious questions answered by experienced professionals with a broad range of expertise. The event was followed by an additional 30-minute Networking and Hors d'oeuvres session, and the business cards were really flying.

The March event, Protection of Consumer Information, was also extremely well received, and received member accolades for the topic(s) covered, quality of speakers, value of the event (6 CPEs and all-day food for \$79), and location! It was held in Walnut Creek, and the event sold out for its capacity of 80 attendees a week ahead of time! This was a full-day event that covered several facets to the Protection of Consumer Information, including The Standard of Care, OECD Fair Information Practices Policy Framework, PCI DSS Framework, Incident Response, Consumer Notification and Mitigation of Injury, and Industry Issues and Standards. Look ahead for more all-day events and different event locations around the Bay Area!!!

For the remainder of the year, we are committed to continuing the strong momentum we have built by putting member feedback into action, and are looking to have an additional "Core Competency" session in May on the importance of Database Auditing. One of this year's remaining events is slated to be another full-day event, and we are hoping to offer members an excellent way to earn CPEs at bargain prices. Here is a sneak peak at the events we are planning for the remainder of the year:

Month	Topic
May	DB Security, Risks, and Auditing ('Core Competency' session)
June	Soft Skills and Employability 'Tune-Up' (Full-Day Event)

As events and dates become finalized, we'll be sure to keep you informed every step of the way.

If you missed our previous events so far, below is a quick re-cap. We hope you join us at our next event.

EDUCATION MESSAGE CONT'D

Month	Topic	Speaker(s)
October 2008	Business Continuity Management Standard BS25999: The BIG Picture	Lee Milligan - Sr. Project Manager, SunGard Availability Services
November 2008	Avoiding HIPAA Pitfalls: An Auditor's Guide to the Regulation of Healthcare IT	Bill Pankey - Partner, Tunitas Group
December 2008	Member Appreciation Event	N/A
January	Computer Forensics Panel	Juan Rivera - Information Systems Security Officer (ISSO), U.S. Coast Guard / D.H.S. Brian Robson - Information Security Professional, U.S. Coast Guard Intelligence Division John Steensen - President, Spatial Dynamics Corporation Albert Lihalakha - Manager, Forensics Practice - KPMG LLP
February	IS Policies and Procedures: Relevance, Best-Practices, and Compliance Considerations ('Core Competency' session)	Harshul Joshi - Director of IT, CBIZ MHM, LLC
March	Protection of Consumer Information (Full-Day Event)	The Standard of Care - Ann Geyer, Partner – Tunitas Group OECD Fair Information Practices Policy Framework - Barbara Lawler, Chief Privacy Officer – Intuit Inc. The PCI DSS Technical Framework Panel - Mark Lundin, Partner – KPMG LLP; Niall Browne, CISO – LiveOps; Harshul Joshi, Director – CBIZ MHM, LLC; Shafeeq Banthanavasi, Senior Manager – Deloitte Incident Response, Consumer Notification and Mitigation of Injury - Kieran Norton, Senior Manager – Deloitte Industry Issues and Standards - Mark Lundin, Partner – KPMG LLP
April	Cloud Computing Panel (Joint event with itSMF)	Subra Kumaraswamy CISSP, Senior Security Manager - Sun Microsystems Stephen Carn, Senior Operations Manager - VMC Inc. Doron Rotman, National Privacy Service Leader, KPMG LLP Anand Ganesan - Solution Architect Patrick Heim - Chief Information Security Officer, Kaiser Permanente (Moderator)

2009 BEST PAPER CONTEST

SAN FRANCISCO ISACA CHAPTER PRESENTS 2009 SPRING BEST PAPER CONTEST FOR PROFESSIONALS MAY 19, 2009 – JUNE 19, 2009

AWARDS

1st Place – \$300.00 will be awarded to the author of the winning paper; the winning paper will also be published in the San Francisco ISACA Newsletter and on the San Francisco ISACA Chapter Website; and the winning paper will be submitted for publishing to the *ISACA Journal* subject to the *ISACA Journal* terms and conditions.

2nd Place – \$200 will be awarded to the author of the second place paper; the paper will also be published on the San Francisco ISACA Newsletter and on the San Francisco ISACA Chapter Website.

3rd Place – \$100 will be awarded to the author of the third place paper published on the San Francisco ISACA Chapter Newsletter and on the San Francisco ISACA Website.

All winners will be recognized at the Annual General Meeting of the San Francisco ISACA Chapter.

ENTRY SUBMISSION DEADLINE

All submissions must be received by 11:59PM on Friday, June 20, 2009.

HOW TO PARTICIPATE

Complete a registration form from the San Francisco ISACA website: <http://www.sfisaca.org>.

See the registration form for topics, submission information, and guidelines.

Please direct any further inquiries to bpc09@sfisaca.org

2009 BEST PAPER CONTEST

MAY 19, 2009 – JUNE 19, 2009

REGISTRATION FORM

Name: _____
(first) (last)

Organization: _____

Address: _____

City: _____ State/Province: _____ Postal/Zip Code: _____

Country: _____ Telephone: (_____) _____ Fax: (_____) _____

Email: _____ (include country and/or area code with telephone & fax)

GUIDELINES

- 1) Submit this form by email to the contact below.
- 2) Write a paper consistent with all requirements set forth in this document.
- 3) Submit the paper electronically by 11:59PM on Friday, June 19, 2009 to bpc09@sfsaca.org.

TOPICS

Authors should cover either new developments in the field or in-depth technically oriented subjects. Major features should have broad appeal and focus on practical matters; purely theoretical material is not solicited.

TYPES OF ARTICLES

Articles may be factual recitations of research or experiential findings, or they may express the author's opinion on a topic pertinent to IS professional readers. (Opinion articles will be clearly identified as such.) Articles should be from four to ten double-spaced pages in length. Articles may be edited for length and appropriateness of content for our readers. A strong article will commingle the pertinent facts with references to personal experience, and use anecdotes to illustrate the author's key points. Quotations from other experts involved also add to the article's depth. Please obtain quotes and add perspective from as broad a mix of countries as possible, in recognition of the international nature of the IS professional readership. The use of references and/or endnotes is strongly encouraged, as they increase the relevance and significance of an article and increase its relevance to the industry's general body of knowledge.

Articles based on surveys or questionnaires must indicate when and where the study was done, relate the number of respondents, and include a brief analysis of the results and an evaluation of the significance of the results.

Authors are strongly encouraged to include exhibits, graphics and artwork for an article. They will assist the reader in comprehending and retaining the information in your article. Such items are treated as text manuscripts requiring the same warranties and assignments. Art files should be submitted separately from the text, in jpg, tif or gif format.

SUBMISSION REQUIREMENTS

The following guidelines must be followed when formatting a document for submission:

- Electronic submissions in Microsoft Word are preferable.
- However, hard copy that is typewritten, double-spaced between paragraphs, one-sided, and on 8 ½" x 11" or A-4 paper will be accepted for the review process. If the article is accepted, an electronic file will be required.
- These documents parameters must be followed:
 - Turn off the hyphenation.
 - Double-space lines.
 - Number pages in the upper right corner.
 - Turn off the right justify option.
 - Do not use automation headers/footers.
 - Turn off track changes.
 - Select standard printer specs.
 - Avoid special characters or keys. (For example, for indents use the TAB rather than the indent key.)
- Article length should be from four to ten pages, double-spaced. Articles may be edited for length and appropriateness of content for IS professional readers.
- Use endnotes at the end of the article, rather than footnotes, to credit sources.
- Include a reference section for any and all general references.
- Include a brief biography including current position, background, professional affiliations, and books or articles published.

2009 BEST PAPER CONTEST

REVIEW PROCESS

Manuscripts are subject to review by two or more IT audit professionals designated by the San Francisco ISACA Board of Directors. The three highest ranked papers meeting the requirements noted above will be selected to receive the awards. The winning article published in the San Francisco ISACA Newsletter and website becomes part of the San Francisco ISACA's overall copyright, as specified in the Author Warranty and Copyright Assignment form that authors are asked to sign.

Manuscripts for publication in the San Francisco ISACA Newsletter and website are edited for grammar and according to The New York Times Manual of Style and Usage and the Merriam Webster's Collegiate Dictionary (www.webster.com). Significant content revisions are returned to the author to be made.

AWARDS

1st Place – \$300.00 will be awarded to the author of the winning paper; the winning paper will also be published in the San Francisco ISACA Newsletter and on the San Francisco ISACA Chapter Website; and the winning paper will be submitted for publishing to the *ISACA Journal* subject to the *ISACA Journal* terms and conditions.

2nd Place – \$200 will be awarded to the author of the second place paper; the paper will also be published on the San Francisco ISACA Newsletter and on the San Francisco ISACA Chapter Website.

3rd Place – \$100 will be awarded to the author of the third place paper published on the San Francisco ISACA Chapter Newsletter and on the San Francisco ISACA Website.

COPYRIGHTS AND REPRINTS

The San Francisco ISACA® Chapter obtains first international serial rights to any published manuscript in the San Francisco ISACA Newsletter and website on behalf of the submitter. While every effort is made to preserve the author's (or authors') style, the San Francisco ISACA Chapter and the San Francisco ISACA Communication Committee reserve the right to edit articles. The San Francisco ISACA Chapter and the San Francisco ISACA Communication Committee reserve the right to publish at their sole discretion.

The San Francisco ISACA Best Paper Contest predominantly accepts original manuscripts. However, in some cases, finished manuscripts also will be considered. Advertising and public relations agency submissions are considered only if the submissions are objective, balanced and cite examples from US as well as non-US countries.

Each article published in the San Francisco ISACA Newsletters and website becomes part of the San Francisco ISACA's overall copyright, as specified in the Author Warranty and Copyright Assignment form that authors are asked to sign.

SELECTED TOPIC FOR SUBMISSION AND CERTIFICATION

I hereby select the following topic to submit under this contest _____

_____.

I hereby agree that any documents submitted by me for this competition will thereby be the property of ISACA SF Chapter; and that I have read and I agree to the above.

Signature: _____

Please print your name _____

REMINDER ABOUT THE CHAPTER'S EMAIL OPT-OUT POLICY

In the past, when we received requests from members to have their email addresses removed from the SF ISACA mailing list, we respected the requests and did just that. But because we receive member information from ISACA International on a monthly refresh basis, continuing to maintain opt-out preferences locally has become a process that SF ISACA is unable to support. Therefore, the chapter decided to discontinue the maintenance of opt-outs.

Please note that, despite this change, we are continuously thinking of ways to improve the member communication process. We also work hard to limit the number of messages we send to our members, reserving that communication channel for internal chapter business only, and not for cross promotion for other organizations or events.

The only way to ensure that you don't get messages from SF ISACA is to contact ISACA International and ask for your email address on file be deleted (email address is a required field on the member profile page, so you can't remove it yourself). Since SF ISACA receives member information from ISACA International, if your information comes in with a null email address, then no message will go out from us. Note that this process would also eliminate messages from ISACA International.

For more information regarding the chapter's communication policy, please visit our web site at <http://sfisaca.org/index.htm> and go to "About Our Chapter."

MEMBERSHIP MESSAGE

New members since February 26, 2009

Aaron Aubrecht
Francis Joseph Barthelom
Stephanie Craig
Lisa Graef Davis
Carol Dippel
Colleen M. Dunn
Karen Gebhart
Jing Ying Kuang
Kathy Fong Lau
Alice M. Leon
Carmen Leung
Scott Marshall
Kyle William McKenzie
Dominique V. Nguyen
Henry I. Olson
Timothy L. Philpott
Ravi Randhawa
Daniel J. Souza
Tung T. Tran
Peter G. Van de Mortel
David Rodrigo Martínez Zamora

Transfers to SF Chapter since February 19, 2009

Tony Castillo
Joe Dupre
Gina Gardiola-Chin
Nancy A. Gonzales
Himanshu Gupta
Kenny Hong
Robert Joseph Otten
Binita Pradhan
Srivastava Prakhar
Swetha Rao
Patrick J. Roberts
Cameron Smith

CISAs and CISM's Working in Sync: How Their Individual Contributions Together Can Achieve Effective IT Risk Management By Vito Sardanopoli, CISA, CISM, CISSP

As most, if not all, readers of the Journal would agree, many organizations benefit from the contributions made by professionals who have achieved the Certified Information Systems Auditor (CISA) and/or Certified Information Security Manager (CISM) certifications. Based on current levels of demand for such professionals, opportunities for experienced CISAs and CISM's are expected to continue growing.¹ As a product of this growth, there is an increased likelihood that CISAs and CISM's will cross paths even within the same organization. Should conflict be expected between CISAs and CISM's due to their closely related areas of focus? What can the CISA and CISM do to ensure they work together productively while minimizing conflicts?

CISA—An Established Veteran

With the CISA certification established nearly 25 years earlier than the CISM, CISA has some obvious advantages, such as greater worldwide recognition. However, a great deal has changed since CISA was originally established. The information technology (IT) audit profession underwent considerable changes in the late 1980s and early 1990s to adapt to the advent of client-server computing along with the move away from mainframe computing. The IT auditor was relied upon more heavily to review and validate controls and recommend improvements. With the incorporation of the Internet into the business models of organizations, being able to achieve and maintain the CISA certification took on another dimension.

These technology developments make the goal of achieving effective IT risk management an even greater challenge. These changes resulted in an increasingly complex technology environment within which IT risks would need to be continually identified and evaluated and either reduced or eliminated where possible. As a result, this presented an obvious opportunity for the highly qualified CISA to make meaningful, even vital, contributions to IT risk management. However, the CISA would now be required to address a broader spectrum of risks stemming from the use of technologies that are increasingly varied and complex. The CISA now must possess a broader spectrum of technical knowledge and skill to maintain a high level of effectiveness.

However, the overall purpose of the CISA's role—to evaluate IT risks and recommend ways to address them—has essentially stayed the same. What has changed is what is required for the CISA to fulfill that role successfully.

Another important means by which organizations adequately address IT risk management is security. The many components of security, e.g., passwords, identity management, encryption, vulnerability monitoring and prevention, primarily serve two basic needs:

1. Reduce or mitigate identified risks
2. Help to avoid anticipated or potential risk

A CISA must ensure that sound IT controls are in place. These controls often consist of, or are dependent upon, IT security measures of various forms. Therefore, it is becoming more of a reality that the CISA, to be capable of ensuring the presence of proper controls, must be able to comprehend IT security to a certain degree. It is probably safe to say that a considerable and growing portion of a CISA's success is dependent upon his/her ability to grasp IT security concepts. Additionally, it is likewise beneficial for the CISA to have at least some experience with hands-on technology tasks. While not an outright requirement, such hands-on exposure can contribute to the CISA's effectiveness as an auditor.

The fact that the CISA has a long track record of success results in both pros and cons. Overall, CISA is more widely recognized than CISM. That awareness contributes in some degree to a CISA's success. On the other hand, CISA's longer history may be viewed by some as a liability. It is expected, and required, that once one achieves the CISA certification, the individual will continue to maintain a high level of knowledge and expertise to keep up with changes. As organizations strive to maintain or grow their businesses, the CISA is expected to adapt to new technologies, regulations, methods and industry best practices.

Some CISAs, particularly those with a body of work exclusively within the IT audit and assurance arena, may find keeping up with such changes difficult.

Nevertheless, a CISA who does not progress in his/her career through the technical ranks can still be highly effective and successful. His/her focus will be to establish and/or improve internal IT-related controls for the purpose of eliminating or minimizing IT-related risks. In many instances, deep technical knowledge or extensive hands-on technical expertise is not required to accomplish this effectively. In cases where technical knowledge or skill is needed, the CISA can research the particular technology involved and have frank discussions with those individuals responsible for performing and implementing the technical measures to address identified risks. For example, an IT auditor holding the CISA designation may determine that any modifications to a critical Oracle production database containing highly sensitive corporate data be logged and

WORKING IN SYNC CONT'D

actively monitored. Such a recommendation in and of itself may be appropriate; however, the CISA can add further weight to his/her recommendation by suggesting Oracle-specific measures (e.g., configuration settings, use of built-in utilities, acquisition of third-party tools) that can be used to accomplish such auditing and monitoring effectively. By taking that additional step, the CISA can earn greater credibility within the organization and help facilitate the implementation of the recommendations.

CISM—A Relative Newcomer

Although the CISM certification is relatively new, the genuine need for management and leadership of the security function has become more evident. Some organizations are only now formalizing the security function. On the other hand, there are many organizations, such as long-established companies within the financial, information services and e-commerce industries, that are refining already-established security functions. In many, if not most, of these organizations, the varying scenarios of the state of information and IT security have a common thread: the reality that information security is maturing to an increasingly essential function with an importance that will only continue to grow. This current scenario presents formidable opportunities and challenges for the CISM.

What is especially important to note is that the CISM certification serves a related but different purpose from the CISA: a means to demonstrate leadership and management experience and expertise within the information and technology security profession.

With that in mind, how should the CISA and CISM view and work with one another?

CISAs and CISM: Conflicting Scopes or Seamless Interaction?

Due to the closely related nature of their scope and responsibilities, the CISA and CISM, although each unique, are increasingly requiring interaction with one another.

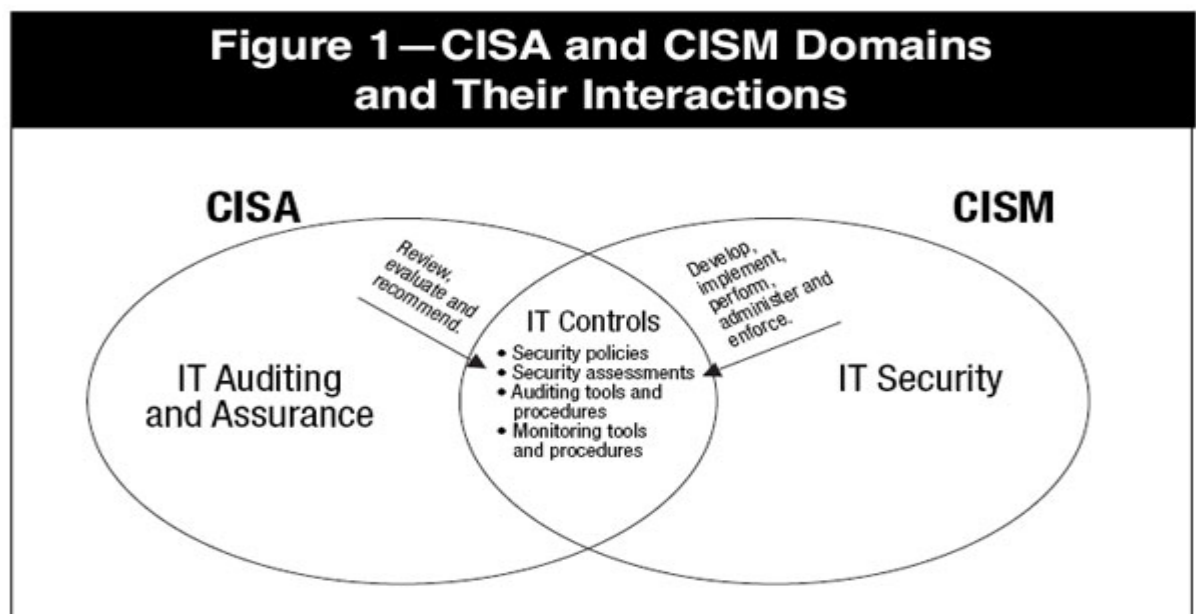
The obvious fact that both the CISA and CISM should acknowledge is that their unique contributions are essential for their organization to effectively address IT risk management. Rather than being at odds with each other, the CISA and CISM should recognize how their efforts

should complement one another.

Although there likely will be exceptions, generally the CISM will be focused on developing, implementing, enforcing, and administering or performing security measures (i.e., through tools, procedures and assessments) that impact specific IT risks directly or indirectly. These measures could be implemented in the context of overall IT strategic planning or to address known vulnerabilities.

The CISA, on the other hand, is focused on periodically and systematically evaluating key IT risks and making recommendations on how to mitigate such risks. This would include evaluating security measures in place and making appropriate recommendations accordingly.

Together, the CISA and CISM share a common goal: to mitigate unacceptable risks and manage residual, acceptable risks on behalf of the enterprise (figure 1).



For example, a corporate security policy governing remote access to enterprise networks and systems would typically be developed by a corporate function (e.g., information or IT security, IT security governance, IT risk management) under the direction of a CISM. An internal or external auditor, likely a CISA, would be responsible for evaluating the quality and completeness of that policy for the organization as well as testing to ensure compliance. By sharing a common goal—maintaining an effective remote access security policy for the organization—the CISA's and CISM's individual efforts actually reinforce one another. Ideally, these efforts should have a synergistic impact on achieving their common goal.

By the CISA and CISM working diligently to support each other's efforts, together they can help to communicate to and execute at all levels of the organization their efforts to address IT risk management. Doing so will not only help to support future efforts of the CISA and CISM to make improvements, but will also help demonstrate that their efforts are valuable contributions to the success of the

WORKING IN SYNC CONT'D

enterprise. For the CISA and CISM to maximize the impact of their work, they must acknowledge each one's scope and responsibilities, identify their common goals, and jointly strive to reach those goals.

Conclusion

For the CISA and CISM to continue the success and progress of their respective certifications and roles, they will need to keep close tabs on the evolution of the IT audit and IT security functions, respectively. Just as important, to better ensure the effectiveness of their unique contributions to the enterprise, they will need to maintain awareness of each other's primary focus, objectives and strengths. This will help them continue to seek opportunities to work together peacefully and productively and, ultimately, synergistically.

Endnotes

1 Wunder, Sarah Stone; "ISACA Certs: Continuing to Grow in Demand and Importance," Certification Magazine, November 2006, www.certmag.com

Vito Sardanopoli, CISA, CISM, CISSP is an experienced IT executive whose responsibilities have encompassed managing multiple functions within IT. He is former head of security at The American Stock Exchange, Rabobank International and PDI Inc., and US group head of IT audit for London-based United Business Media PLC.

The above article was reprinted from Volume 2, 2008 of the ISACA Journal with ISACA International's permission.

SAVE THE DATE: September 21, 2009 – September 23, 2009



KEYNOTE SPEAKER:

Randall N. Spratt

**Executive Vice President, Chief Information Officer
McKesson Corporation**



Randall N. ("Randy") Spratt is Executive Vice President and Chief Information Officer for McKesson Corporation. Spratt is responsible for McKesson's global technology strategy and technology infrastructure operations for the Corporation. A passionate executive with a strong

emphasis on sound governance, good process, and constant innovation, he is leading the evolution of McKesson's information technology as a competitive edge in every business line.

Spratt has been with McKesson for more than 20 years, most recently as chief process officer for McKesson Provider Technologies (MPT), the company's medical software and services division based in Alpharetta, Georgia. He also managed MPT's Business Development, Information Technology, and Strategic Planning offices, as well as MPT's Technology Services business.

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

Priced at \$525 (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 2009 SF ISACA Fall Conference features four tracks:

1

Core Competencies: Focuses on teaching the IT Audit basics. Target audience: New IT Auditors, Financial Auditors, those who Manger IT Audits or IT Auditors, as well as IT Operational and Security Personnel wanting to learn more about IT Audit and Governance.

2

Strategies & Techniques: Builds on the basics. Target Audience: Anyone wanting to learn more about the strategies, techniques, and tools used in IT Auditing.

3

Compliance & Governance: Various topics regarding compliance and governance that will range from intro courses to in-depth thoughts and guidance. Target Audience: Anyone wanting to learn more about how compliance and governance impact their organizations and their audits.

4

In-Depth Technical: Longer courses (typically day-long) that dive deep into technical topics, usually involving demonstrations. Target Audience: Intermediate to Advanced IT Auditors.

In addition to the educational sessions, the 2009 SF ISACA Fall Conference will also feature an **Exhibitors Hall** and **Exhibitors Lunch** on Tuesday, September 22nd where you can learn more about the products and services of the firms that help sponsor the conference. 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 system will be open in June.

Make your plans to attend today!

SAN FRANCISCO CHAPTER BOARD ROSTER 2008 - 2009

**EXECUTIVE BOARD
PRESIDENT – NOMINATION
COMMITTEE CHAIR**
CONNIE CHENG, SAN DISK
CONNIE@MLEMIEUX.COM

**1ST VICE PRESIDENT – CISA
WORKSHOP CO-COORDINATOR**
VIKRAM PANJWAN,
PRICEWATERHOUSECOOPERS
OFFICE: (415) 498 7332
VIKRAM.M.PANJWANI@US.PWC.COM

**2ND VICE PRESIDENT –
MEMBERSHIP CO-CHAIR AND
COMMUNICATIONS CO-CHAIR**
STEVE OWYOUNG, KPMG
OFFICE: (415) 963-7603
SOWYOUNG@KPMG.COM

**SECRETARY – POLICIES AND
PROCEDURES CO-CHAIR**
AL LAVASSANI, WELLS FARGO
OFFICE: (415) 371-5849
AL.LAVASSANI@WELLSFARGO.COM

**TREASURER – FALL CONFERENCE
CO-CHAIR**
TIM STAPLETON, WELLS FARGO
OFFICE: (415) 283-5937
STAPLETI@WELLSFARGO.COM

IMMEDIATE PAST PRESIDENT
KEVIN FRIED, DELOITTE & TOUCHE
OFFICE: (415) 783-4639
KEFRIED@DELOITTE.COM

**DIRECTORS / CHAIRS
DIRECTOR**
MARY T. LEE
MTL0828@COMCAST.NET

DIRECTOR – CGEIT COORDINATOR
DEBRA MALLETTE, KAISER PERMANENTE
OFFICE: (510) 627-3626
DEBRA.MALLETTE@KP.ORG

DIRECTOR – EDUCATION CO-CHAIR
HEATHER OUELLETTE, KPMG
OFFICE: (415) 963-7237
HOUELLETTE@KPMG.COM

**DIRECTOR – FALL CONFERENCE
CO-CHAIR**
STEVE SHOFNER, KAISER PERMANENTE
OFFICE: (510) 267-4865
STEPHEN.R.SHOFNER@KP.ORG

DIRECTOR
TODD WEINMAN, THE WEINMAN
GROUP, LLC
OFFICE: (510) 835-3053
TODD@WEINMANGROUP.COM

**DIRECTOR – CO-CISM WORKSHOP
COORDINATOR AND MARKETING
CO-CHAIR**
CHRISTINA CHENG, GOOGLE
OFFICE: (650) 253-1889
CHENGCG@GOOGLE.COM

DIRECTOR
SANDY LEE, PG&E
OFFICE: (415) 973-0161
SEL5@PGE-CORP.COM

COMMUNICATIONS CO-CHAIR
PAULINA FRASER, ADOBE
OFFICE: (408) 536-6639
PTROICKA@GMAIL.COM

**MEMBERSHIP CO-CHAIR –
WEBMASTER**
MIKE NELSON – LOGYX, LLC
OFFICE: 925-413-9779
MNELSON@LOGYX.COM

**CISA WORKSHOP CO-
COORDINATOR**
JIM LUCAS, WELLS FARGO
OFFICE: (415) 396-7585
JIM@LOUKAS.COM

**CISA WORKSHOP CO-
COORDINATOR**
GRIGORI BARBACHOV
GRIGORI_B@YAHOO.COM

**CISM WORKSHOP CO-
COORDINATOR**
ASHOK KUMAR, KPMG
OFFICE: (415) 963-7526
ASHOKKUMAR@KPMG.COM

EDUCATION CO-CHAIR
THEJ MEHTA, KPMG
OFFICE: (415) 963-7738
TMEHTA@KPMG.COM

VOLUNTEER CHAIR
STEVEN MAJOURAU
SMAJOURAU@AOL.COM

ACADEMIC RELATIONS CO-CHAIR
SIMI SOHI, DELOITTE & TOUCHE
OFFICE: (415) 783-6991
SSOHI@DELOITTE.COM

ACADEMIC RELATIONS CO-CHAIR
KESHAV MALANI, DELOITTE & TOUCHE
OFFICE: (415) 783-6990
KMALANI@DELOITTE.COM

**POLICIES AND PROCEDURES CO-
CHAIR**
CARRIE DENG, DELOITTE & TOUCHE
OFFICE: (415) 783-5125
XDENG@DELOITTE.COM

MARKETING CO-CHAIR
SUMIT KALTRA, GRANT THORNTON
SUMIT.KALTRA@GT.COM

**CHAPTER HISTORIAN – POLICIES
AND PROCEDURES CO-CHAIR**
BILL DAVIDSON
WZDAVIDSON1@COMCAST.NET



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

FIRST CLASS
U.S. POSTAGE
PAID
PERMIT NO. 11882
SAN FRANCISCO CA