

## PRESIDENT'S MESSAGE



Todd Weinman  
President

### Hitting our Stride for an Outstanding Year!

Welcome to our first newsletter of the 2001-2002 Chapter year, and my first as President of the San Francisco Chapter. Although our Chapter year just started in July, we have actually been hard at work for many months in planning and preparation for what I believe will be a truly remarkable year for our members. We have many changes, new events, and new initiatives in store for you.

Perhaps the most significant changes are in the area of education. Most notably, in September, we will be presenting our first ever multi-day, multi-track seminar, the 2001 eXciting Fall Seminar (find more information on the seminar elsewhere in this issue). This seminar, which we hope to become an annual event, is a cornerstone of our most important chapter mission: to provide reasonably-priced education events for our members. The seminar will feature tracks in fundamentals, security and hot topics. We have lined up an excellent slate of topics and presenters.

In addition to the multi-day seminar, we will continue to hold a number of full-day technical seminars throughout the year, interspersed with our chapter luncheons. Both the fall multi-day seminar and the full-day technical seminars are a response to member feedback that, in our geographically-dispersed region, many members have difficulty attending chapter luncheons. One of the more interesting full-day seminars will be held in November, when attendees will actually be able to visit one of our member audit departments at the Bank of America facilities in Concord to see first hand how a cutting-edge audit group deals with the issues of Call Centers and Optical Networks.

*Winner of the 2000 Wayne K. Snipes Award –  
Best ISACA Chapter in the USA and the World*

*Winner of the 1999 and 2000 Newsletter Contest –  
Best Newsletter for Large Chapters in North America*

During uncertain economic times, certification becomes more important than ever. The Chapter will continue to host our CISA Review prep course in the months leading up to the CISA exam, presented annually in June. This past year we had one of our biggest classes in years.

The excitement will culminate in May when we host the 2002 North American CACS conference, the largest conference in the world for IS auditors. The last time San Francisco hosted the CACS conference, in 1997, we hosted the largest CACS ever. We look to post a new record in 2002.

All in all, we have an extremely ambitious year planned for our members. The execution of this agenda requires one essential variable: volunteers. There have been times during the last couple of years where we have not always executed as well as we would like. The biggest reason for this is that our volunteer base had dwindled significantly and we had too few people doing too many tasks. Over the past several months we have worked very hard to increase our volunteer base and beef up our committees. But we still have a need to get more of our members to volunteer to support chapter activities. If you have an interest in getting involved, please feel free to contact me (my contact information is at the bottom of this column). While we are on the subject of volunteers, I would like to acknowledge a few of the individuals whose contributions to the chapter over the past several months have been particularly notable.

Certainly, one individual that has been a giant contributor to the chapter over the past several months has been Steven Hudoba, our current 2nd VP and Education Chair.

## PRESIDENT'S MESSAGE – continued

---

Steven may be new to the Bay Area, but his is certainly no stranger to ISACA, having been heavily involved with the Minnesota Chapter for many years, including two years as President. When Steven moved to the Bay Area this past year, I wasted no time in recruiting him for our Board of Directors. No two ways about it, Steven has been a workhorse. Not only has he taken over the intense role of Education Chair, including leading the planning for our 2001 eXciting Fall Seminar, but he has been heavily involved in almost every area of chapter business, and he has brought leadership, experience, and many new ideas to our Board of Directors.

Along with Steven, kudos must go out to the whole Education Committee. When Steven first proposed the idea of holding a three-day multi-track seminar for the fall, I thought he had lost his mind. Thanks to the steadfast work of his committee, we have put together an event that I think has surpassed all of our expectations. Those Education Committee members are Deb Frazer, Mary Laude, and William Luk as well as Rick Beckman and Stuart White, both of whom are on the Board of Directors this year and have made substantial contributions to the committee.

Another outstanding chapter volunteer has been our 1st VP and Communications Chair, Justin Gibson. Justin has played a key role in the overall planning efforts for this coming year in addition to taking on one of our most challenging roles in leading our Communication Committee. His efforts in this area are particularly notable given that we are having to reinvent many of our processes in this area.

Every good baseball team has a utility fielder, a player that can come in and play a variety of positions. Our utility infielder has clearly been Sumit Kalra. Earlier this year, Sumit stepped into our 1st VP role when that position was vacated mid-term. He stepped up and produced our last newsletter. This included performing the desktop publishing, which he had never done before. He has also been a valuable member of our Web team, helping execute timely edits to the Web site. This year he will be taking over responsibilities for our CISA Review course.

Other contributions of note include Beverly Davis, who has provided outstanding leadership to our 2002 CACS committee, including serving as a wonderful ambassador promoting our event at the recent CACS Conference in

Orlando. Karina Daza put in tireless efforts in leading this year's CISA Review course. Treasurer Christina Cheng's efforts enabled us to pass a budget at our first Board meeting in July, months earlier than had been accomplished in recent years. Brian Alfaro has been a strong contributor on the Web team, helping execute numerous updates and changes to the Web site. Brian will also be serving as our Academic Relations Chair this year.

These are not the only contributors, just some of the most notable ones. I hope to see some of your names in this column as the year unfolds. When it comes to volunteering for the chapter, the more the merrier. I also look forward to seeing you at our many chapter events this year.

Todd Weinman, CES  
(510) 232-4264, ext. 17  
todd\_weinman@yahoo.com

---

## EDUCATIONAL EVENTS INCENTIVE AWARDS

This year, we are planning a unique program for participants of our educational events to recognize their support and attendance. While the details of this program are being finalized, we plan to hold a drawing at our April 2002 Chapter Luncheon for the awards. Participants at our educational events will get entries to the drawing based on their attendance during the year. The more events you attend, the better chance you have to win. Watch our Web site for further details as the program is finalized, and be sure to register for our 2001 eXciting Fall Seminar.

*Awards may include Chapter promotional items, such as SF ISACA sweatshirts, or discounts on registration fees for the 2002 CACS Conference to be held in San Francisco in May 2002!*

# 2001 EXCITING FALL SEMINAR

---

In this fast-paced, high-tech world in which we live, racing to keep up with the demands placed on an IS Audit professional is an eXtreme challenge.

Well, mark your calendars for an eXtreme educational opportunity on September 19 - 21, 2001. Respected instructors from the industry and public accounting, as well as experts from within the field, will provide valuable information on a wide variety of topics affecting our profession. Three concurrent sessions will be offered focusing on I.T. Audit Fundamentals, I.T. Security, and I.T. Audit Hot Topics. Don't miss this opportunity to join us at the Palace Hotel in San Francisco to learn from, and network with, the best!

## eXciting Schedule of Topics

| I.T. Audit Fundamentals  | I.T. Security   | I.T. Audit Hot Topics   |
|--|---|---|
| <ul style="list-style-type: none"> <li>• Role of I.T. Audit</li> <li>• I.T. Auditing Standards</li> <li>• Documenting I.T. Systems</li> <li>• Auditing Application Controls</li> <li>• Auditing I.T. General Controls</li> <li>• I.T. Audit Related Topics</li> <li>• I.T. Audit Tools</li> <li>• Audit Software</li> <li>• Building an e-Business Security Framework</li> <li>• Business Continuity Planning</li> </ul> | <ul style="list-style-type: none"> <li>• Windows NT Security</li> <li>• Windows 2000 Security</li> <li>• Auditing A/S400</li> <li>• Electronic Payment Systems Security</li> <li>• Building an e-Business Security Framework</li> <li>• Auditing Cisco Routers</li> <li>• Security Practices for Network Applications</li> <li>• Cracking WEP Keys</li> <li>• Auditing Firewalls</li> </ul> | <ul style="list-style-type: none"> <li>• Network Perimeter Security Architecture</li> <li>• Intrusion Detection</li> <li>• Attack and Penetration Techniques</li> <li>• SAP R3 Security</li> <li>• Auditing Oracle Financials Module</li> <li>• Web Application Level Security &amp; Audit</li> <li>• PKI &amp; Certificate Authorities</li> <li>• Auditing Certificate Authorities</li> <li>• Building an e-Business Security Framework</li> <li>• Social Engineering</li> </ul> |

Note: schedule of speakers and topics is subject to change!

For more information and to register for the 2001 eXciting Fall Seminar, see our Web site at: [www.sfisaca.com](http://www.sfisaca.com).

eXtreme Educational Value – nowhere else can you receive such high quality training at this low price

| 3-Day Event (includes Chapter Luncheon)*                                   | Daily Registration Fee*  | Chapter Luncheon Only*   |
|--|--|--|
| \$500 Members (or 16 Saverpasses)<br>\$600 Non-members (or 20 Saverpasses) | \$225 Members (or 7 Saverpasses)<br>\$250 Non-members (or 8 Saverpasses) | \$40 Members (or 1 Saverpass)<br>\$50 Non-members (or 1 Saverpass + \$10)<br>\$20 Students |

### \* Early Registration Discounts

Participants who register early are entitled to the following discounts. Registrations must be mailed in (postmarked no later than September 1, 2001) to the Chapter with payment in full (checks or Saverpasses only).

- \$50 discount for 3-Day Event
- \$25 discount for Daily Registration
- \$5 discount for Chapter Luncheon

# HOW TO WRITE A COMPUTER SECURITY POLICY

sponsored by the  
Henderson Group  
Computer Security  
Consulting and Training

## About Stu Henderson:

Mr. Henderson is an experienced consultant who specializes in effective computer security for IBM mainframes and Windows NT/2000.

He has helped hundreds of organizations make better use of security software such as RACF, ACF2, and TopSecret. He has conducted MVS security reviews for numerous commercial and government organizations.

He communicates effectively with all levels of staff, from computer operator to executive management.

He has over twenty-five years of hands-on experience as a system programmer, Data Security Officer, and consultant, culminating in his founding his own consulting organization, the Henderson Group. He can be reached at (301) 229-7187.

His Web site is  
<http://www.stuhenderson.com>

## Where To Get More Info

- The RACF User News (for a free subscription, call (301) 229-7187)
- The Computer Security Institute, (415) 905-2370
- The ISPN News, (508) 879-7999

## Help Improve This Paper

This is edition 2 of this document. Many companies and individuals have contributed ideas to it. Your company will likely find additional points and suggestions from which others could benefit. Why not share them with others? We will include all valid suggestions in the next edition of this paper. Send them to:

Stu Henderson  
5702 Newington Road  
Bethesda, MD 20816  
Phone (301) 229-7187  
Thanks for your help.

## Introduction

It happens at least once in every company: an employee with little background in the area is assigned the task of developing a computer security policy statement. This paper provides help to that employee by summarizing what other companies have put in their policy statements and how successful policies have been implemented. Each company must decide on its own what its policy will include. The following descriptions provide the rough material from which that tailoring can proceed.

## Why Have a Computer Security Policy Statement?

Policy statements are necessary to make employees aware and to clarify responsibility. Fancy hardware and software will not provide adequate protection unless every employee understands the importance of security, and what the company expects of its staff. A company has a firmer case to terminate or prosecute an offender if the company's policy has been put forth in writing. Finally, the interdepartmental communication which is necessary to develop the policy will help all departments to understand what is needed, what is possible, and what they are responsible for.

## Who Should Develop the Policy?

No single employee should develop the policy. Senior managers of every functional area should be involved in its development. (This gets them to "buy in" and ensures that their knowledge and expertise are incorporated.)

One successful approach is for a manager (the director of data processing may be best) to suggest to his or her peers a task force to develop the policy. If they agree, one employee is assigned to be project manager and editor of the policy. The editor selects points to be included from the following suggestions and lists them in "bullet" form for task force review. As the task force discusses the bullet points and tailors them to the company's requirements, the editor updates the working draft of the statement and

converts the bullets to sentences and paragraphs. In this way managers can participate without taking too much of their time, and the editor has an opportunity to demonstrate his or her skills as a project manager, meeting facilitator, and negotiator. The editor should have some background in data processing, EDP audit, or computer security.

## How Detailed Should the Policy Be?

Detail is less important than thorough coverage. Task force members may not care how the Personnel Department ensures that terminated employees' access privileges are revoked. They do care that the issue is being addressed and that someone is clearly assigned responsibility for it. A good policy won't address every little item. It will however make sure that someone or some department is specifically responsible for developing procedures to handle every important issue.

On the other hand, don't be bothered if procedural details end up in your company's policy statement. They don't detract and you can always change the title to say "Computer Security Policy and Procedures".

## Suggested Outline

Here are some major categories to organize your policy and some items to consider including in each:

### A) Introduction and Purpose

- Our firm depends on its computers, data, and information processing capabilities.
- Description of technical risks of: altered, stolen, inaccurate, destroyed data and loss of ability to process data
- Description of business risks of: suits for not protecting sensitive data, loss of competitive advantage from theft of customer lists and other business assets, liability for incorrect data, incorrect business decisions due to incorrect data, publicity surrounding regulatory enforcement, inability to process business transactions, and other risks.

- Every employee must be aware of these risks and act in a way to protect the firm.
- This policy statement details employees' responsibilities for computer security.

### **B) Scope**

- This policy applies to all employees, consultants, auditors, and temporary help, and to all users of our computers.
- It applies to our mainframes, minicomputers, personal computers, outside timesharing services, outside suppliers of data, LANs (Local Area Networks), and computer workstations.
- It applies to all company data and reports derived from company data.
- It applies to all programs developed on company time, using company equipment, or by company employees.
- It applies to all terminals, communications lines, and associated equipment on company premises or connected to company computers.
- This policy does/does not address each of the following: how users are identified to computers, how each user's identity is verified, physical protection over equipment, physical control over access to data, logical control over access to data, integrity and quality of data, data retention requirements (how long data must be kept according to all relevant regulatory requirements), disaster recovery planning for data processing, business resumption planning for all business units.
- Who is responsible for making sure that all affected parties are aware of the policy.

### **C) Responsibility for Computer Security**

- The Data Security Officer (DSO) is responsible for ensuring that the company has adequate computer security and that this policy is observed.
- Every employee is responsible for protection of our assets, including computers and data.
- Every employee should notify the Data Security Officer whenever he or she sees actions which seem to go against this policy.

### **D) USERIDs and Passwords**

- No one is to be permitted to use company computers without an authorized USERID (user identification).
- To get a USERID requires the approval of an officer, of a department head, of the Data Security Officer, of some other authority.
- Each user is responsible for all activity which occurs on his or her USERID.
- The spelling of each USERID is to be determined by the Data Security Officer, according to a standard designed to meet the spelling and length requirements of every type of computer used in our organization. This standard specifies a maximum length of seven characters, including letters, numbers, and only the following punctuation marks (list of acceptable special characters). The letters in each USERID must be upper case/lower case.
- USERIDs may be revoked (or canceled or suspended) at any time.
- USERIDs will be revoked when an employee terminates or transfers.
- The Data Security Officer may at his or her discretion revoke and/or delete any USERID not used for one hundred or more days.
- USERIDs will be revoked when an incorrect password is entered three times in a row.
- Each user must change his or her password at least every 30 days. Computers are to be programmed to require this.
- Company computers are to be programmed so that only users with authorized USERIDs can access them.

### **E) Employment Practices**

- Every employee, consultant, consultant, and temporary employee should have a copy of this policy.
- All new employees will hear the importance of computer security and their role in it during Orientation.
- Department X will be notified of every employee transfer, promotion, and

termination in order to adjust computer access privileges as needed.

- All employees must sign off that they have read, understand, and accept this policy.
- Personnel is responsible for computer security practices relating to employment. This includes: forms for processing employment and termination, informing supervisors of their responsibilities regarding computer security, addressing computer security in the performance review process, assisting in computer security awareness training, distribution of this policy, and Orientation for new employees.
- When an employee is terminated for any reason, the employee's immediate supervisor is directly responsible for having that employee's computer privileges revoked at once on all computer platforms where the employee has privileges. If necessary, the supervisor should log onto that USERID with a sufficient number of passwords to revoke the USERID. The supervisor is responsible for notifying the Computer Security Department and the Personnel Department when a USERID should be revoked or deleted.

### **F) Access to Equipment**

- Only authorized persons whose work requires it will be allowed access to mainframe computers.
- All computers, terminals, and communications equipment will be protected against fire, water, electric power fluctuations, physical damage, and theft. Protection will be selected from among: physical barriers, environmental detection and protection, insurance, and other means on the basis of both replacement cost and effect on our ability to conduct business.
- Department X is responsible for controlling access to mainframe computers and for providing adequate protection to computers, terminals, and communications equipment.



# HOW TO WRITE A COMPUTER SECURITY POLICY – continued

---

## G) Responsibility of Every Employee

- Computer security is the responsibility of every employee.
- No employee shall divulge company information to outsiders.
- Company computers shall not be used for purposes not related to company business.

## H) Access to Data

- All data files on company computers will be protected against unauthorized changes.
- Sensitive data files will be protected against unauthorized reading and copying.
- The definition of “sensitive” as used here is....
- Company computers shall be programmed to control which USERIDs can read and which USERIDs can write to any given file.
- Every file shall be associated with an owner. Unless otherwise specified, the owner of a data file is the head of the department which paid for the computer programs which created it.
- The owner of each file is responsible for specifying whether the file is sensitive, and which USERIDs should be allowed to read or write to it. Such specification should be in writing, signed by the owner, and routed to the Data Security Officer.
- The Data Security Officer is responsible for ensuring that the access rules specified by data owners are implemented correctly, and that they match the written specification provided by the owners.
- The Data Security Officer will periodically review access rules for data with the data owners, with Legal, and with the Controller to ensure that the rules provide adequate protection.
- Internal Audit is responsible for periodically verifying that the access rules specified by the owners are correctly implemented.

## I) Procedures to Update the Policy

- Who has the authority to change the policy?
- How are changes accomplished?

## J) Online Systems

- Access to an online system (that is, through computer terminals) is allowed only to USERIDs which have been authorized to that system.
- What techniques will be used to control access to online systems and terminals (physical barriers, access control software, dial-back system, automatic shutdown of idle terminals, restriction of sensitive transactions to specified terminals)?

## K) Encryption

- When must data files be encrypted?
- When must passwords be encrypted?
- What encryption techniques are acceptable (DES, RSA public key, or comparable)?

## L) Personal Computers

- Department X is responsible for developing guidelines and procedures for protection of personal computers and the data processed on them.
- When personal computers are connected to telephone lines, they are considered the same as terminals and are to be controlled in the same way as terminals.

## M) Contingency Planning

- Department X is responsible for developing and coordinating recovery plans for all departments in the event of the destruction of our data center and also in the event of short-term loss of any of our data processing capability. These plans should be based upon a systematic assessment of the risk of loss of the ability to process transactions for each application on each platform.

## N) Miscellaneous

- Stealing software is illegal and can serve as grounds for prosecution and termination of employment. (This sentence may protect your company from a suit if one of your employees is accused of software piracy, since he or she will have allegedly done it in violation of company policy. Refer to

- Our company does not permit use or possession of copies of software without paying appropriate fees and signing of appropriate licenses. Department X is responsible for conducting inventories of the software on company-owned personal computers to ensure that no software is on them without proper payment and licenses. (This may protect your organization from SPA (Software Publishers Association) audits conducted by Federal marshals.)
- Department X is responsible for developing guidelines for “spread-sheet audits” or reviews of decision support models to avoid unjustified reliance on computer-generated projections.
- Department X is responsible for providing means to protect access to sensitive computer printouts.

## O) Multi-Platform Security

- Local Area Networks (which are subject to sniffer programs), UNIX workstations, and other platforms in user departments (outside the control of the Data Processing Department) are considered not to have rigorous physical security and logical security. Because of this, any such platforms which are to be connected to the company’s network must comply with the company’s plan for third-party authentication or other means to support multi-platform security. Department X is responsible for researching and coordinating such a plan. This plan should include the means to standardize the spelling of USERIDs across all platforms, so that each user needs to remember only one USERID.

## P) Internet Access

- Access to the Internet from company premises or equipment is permitted only under the guidelines and supervision of Department X, which is responsible for developing, documenting, and disseminating such guidelines.

## CALENDAR OF UPCOMING EVENTS

| Date                  | Event  | Place   | Cost   |
|-----------------------|--|---|--|
| July 18, 2001         | Economic Espionage, Counterintelligence and Cybercrime. Annual Planning Meeting. | Palace Hotel, San Francisco<br>Luncheon meeting, afternoon planning meeting | \$35 Members<br>\$45 Non-members                                   |
| September 19-21, 2001 | Fundamentals Track, Security Track, Hot Topics Track                             | Palace Hotel, San Francisco<br>Multi-day, Multi-track (3 days)              | \$500 Members<br>\$600 Non-members (early registration saves \$50) |
| October 16, 2001      | Joint IIA/ISACA Luncheon   | Palace Hotel, San Francisco<br>Luncheon meeting                             | \$40 Members<br>\$50 Non-members                                   |
| November 15, 2001     | Optical Networks and Call Centers  | Bank of America, Concord<br>Full day seminar                                | \$110 Members<br>\$135 Non-members                                 |
| December 13, 2001     | Networking Event   | Palace Hotel, San Francisco<br>Holiday Dinner Meeting                       | \$40 Members<br>\$50 Non-members                                   |
| January 17, 2002      | Technical Topic  | Palace Hotel, San Francisco<br>Full day seminar                             | \$110 Members<br>\$135 Non-members                                 |
| March 21, 2002        | Hot Topic  | Palace Hotel, San Francisco<br>Full day seminar                             | \$110 Members<br>\$135 Non-members                                 |
| April 18, 2002        | Networking Event   | Palace Hotel, San Francisco<br>Luncheon meeting                             | \$40 Members<br>\$50 Non-members                                   |
| May 5-10, 2002        | North American CACS 2002   | The Fairmont, San Francisco<br>Full week                                    | \$1,295 Members<br>\$1,445 Non-members                             |

## Member Milestones

|  |   |   |  |
|--|---|---|--|
| Join the Board of Directors in saluting the following long-term Chapter members: | <b>Members for over 20 Years</b><br><b>Robert Abbott</b><br><b>Douglas Webb</b><br><b>Hector Massa</b><br><b>Arnold Dito</b><br><b>David Durst</b><br><b>John Sheehan</b><br><b>Richard Tuck</b><br><b>Charles Cresson-Wood</b> | <b>Members for over 15 Years</b><br><b>William Davidson</b><br><b>Robert Kimball</b><br><b>Joel Lesser</b><br><b>William Martin</b><br><b>Bruce L. Reid</b><br><b>Kathleen Williams</b><br><b>Ronald Rasch</b><br><b>Kerry G. Elms</b><br><b>Harry Lew</b><br><b>Allen Martin</b><br><b>William T. Tener</b><br><b>Frank Yee</b><br><b>Jerry K. Hill</b><br><b>Katherine Ullman</b> | <b>Members for over 10 Years</b><br><b>Ben H. Choi</b><br><b>Marcus A. Jung</b><br><b>Nancy Weisbrook</b><br><b>Eugene Menning Jr.</b><br><b>Paley Pang</b><br><b>Vickie Smith</b><br><b>Guy Anderson</b><br><b>Adam F. Levine</b><br><b>Robert C. Motts</b><br><b>Sharon Tatehara</b><br><b>Ann Y. Lee</b><br><b>I-MEI Chen</b><br><b>Ralph Nefdt</b> |
|--|---|---|--|

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 Justin Gibson, Communications Committee Chair (justin.gibson@us.pwcglobal.com).

## MEMBERSHIP



Hector Massa  
Committee Chairperson

The membership count for the San Francisco Chapter as of July 2, 2001, stands at 330 members. Please join me and the SF ISACA Board in welcoming these Chapter members.

Mahary M. Araia  
Inovant  
Maraia2visa.com

Richard Chase  
Pen-Cal Administrators  
rchase@pencal.com

Shawn M. Davenport  
Currenex, Inc.  
shawn.davenport@currenex.com

Claude Khoury, CPA  
PricewaterhouseCoopers  
claude.khoury@us.pwcglobal.com

Ryan C. Lai  
Federal Reserve Bank  
ryan.c.lai@s.frb.org

Donald R. Saxinger  
Federal Deposit Ins. Corp.  
dsaxinger@fdic.gov

William B. Shaffer  
Providian Financial  
Brad-shaffer@providian.com

Erin L. Andrews, CISA  
PricewaterhouseCoopers, LLP  
Erin.Andrews@us.pwcglobal.com  
*Reinstated member*

Wendy Benedict, CISA  
Providian Financial  
Wendy\_benedict@providian.com  
*Reinstated member*

Richard Buford, CISA, CIA  
Wells Fargo Bank  
bufordr@wellsfargo.com  
*Reinstated member*

Catherine A. Graham,  
CISA, CA, CMC  
San Mateo, CA  
catgra@hotmail.com  
*Transferred from Vancouver Chapter*

Bruce K. Harvey,  
CISA, CFE, CFSA, ASQ  
San Francisco  
bharvey@pacific.net.sg  
*Transferred from Singapore Chapter*

Carol R. Hopkins, CISA  
Providian Financial  
Carol\_hopkins@providian.com  
*Reinstated member*



## NORTH AMERICA CACS 2002

---



Beverly Davis  
CACS 2002 Chair

The news is out and, by all means, it is GOOD NEWS! The North America CACS 2002 conference will be in San Francisco, May 6-9, 2002. We are the Partnering Chapter and there is lots of work cut out for us to roll out the red carpet. Believe it or not, work has already started and it's not too late to get on board.

Our efforts thus far have been quite successful:

### CACS 2001 in Orlando was our first outreach

Chapter representatives delivered a strong message that CACS 2002 is in San Francisco. Handing out Cable Car Pins gave the traditional invitation to come to the city by the Bay and leave your heart in San Francisco.

### ISACA Members have been assigned lead roles

The following members have accepted leadership roles to coordinate conference activities:

- Sponsorship/Exhibits: Beverly Davis
- Special Events/Hospitality: Kathleen Arnold
- Area Promotion/Publicity: Mark Valade
- Volunteer/On-Site Support: Marcus Jung

### The Foundation will host a Golf Tournament

Justin Gibson is the chapter's host for this outstanding event geared towards fundraising in support of technology research and education.

We are still in need of committed volunteers for each of our committees. If you are interested in being involved contact Beverly Davis at (415) 616-2766 or send e-mail to [davisb@fhlsf.com](mailto:davisb@fhlsf.com).

Please join us and help plan CACS 2002 in San Francisco!

## EDUCATION COMMITTEE

---



Steven Hudoba  
Committee Chairperson

The 2001-2002 Chapter year is off and running and the Education Committee has been busier than ever planning for some terrific events. Most notably, we have our biggest event of the Chapter year scheduled in September: our 2001 eXciting Fall Seminar. This event promises to be one of the best training values available on the West Coast for I.S. Auditors. The Fall Seminar will be held over three days, from Wednesday, September 19 through Friday, September 21 2001, features three tracks for participants to choose from, and is very competitively priced.

The Fundamentals track will provide the entry-level I.S. auditor with an introduction to the profession, including detailed instruction in auditing I.S. General Controls and Application Controls, and an overview of many of the related topics in our field. The remaining two tracks, the Security track and the I.S. Audit Hot Topics track, will both provide the more experienced auditor with a great variety of speakers and topics covering many of the most relevant issues facing our organizations today. Take a look at our Web site at [http://www.sfisaca.org/events/Monthly Events/2001September.htm](http://www.sfisaca.org/events/Monthly%20Events/2001September.htm) for further information about and to register for the 2001 eXciting Fall Seminar.

In October, we will be working with the San Francisco Chapter of the Institute of Internal Auditors once again to jointly host an educational event. The details of this event have not yet been worked out, but we expect this will likely be a Luncheon in downtown San Francisco with a featured speaker from the industry on a topic relevant to both IS and financial/operational auditors.

In November, we are delighted to announce that the Bank of America has agreed to host our Full Day Seminar on the topics of Optical Networks and Call Centers. This event will feature speakers from the respective operational areas within the bank as well as the internal audit function and participants will be treated to the unique perspectives of both sides of the operations/audit equation. Additionally, this event will be held

on-site at the Bank of America's Concord facility, so participants will enjoy a first-hand look at the inside operations of the bank.

December will bring about a special Chapter Dinner Meeting with an emphasis on networking in our profession. This event will capture the holiday spirit with a mix of education, entertainment and opportunities to meet and interact with your colleagues in the I.S. Audit profession.

Educational events further down the calendar include Full Day Seminars in January and March, and another Chapter Luncheon in April. Please keep your eyes and keyboards focused on our "Events at a Glance" page (<http://www.sfisaca.org/events/glance.htm>) on the Chapter Web site for updates.

Also, new for this year is our Educational Events Incentive Awards. We are planning a unique program for participants of our educational events to recognize their support and attendance. While the details of this program are being finalized, we plan to hold a drawing at our April 2002 Chapter Luncheon for the awards. Participants at our educational events will get entries to the drawing based on their attendance during the year. The more events you attend, the better chance you have to win. Look for another announcement about this program in the newsletter and watch our Web site for further details as the program is finalized.

And finally, I owe a great deal of thanks to the members of our education committee who have spent many hours working diligently to put these programs together for you. Please join me in applauding: Rick Beckman (Bank of America), Stuart White (VISA International), William Luk (Wells Fargo), Deb Frazer (APL Lines), and of course, Todd Weinman (Lander International) and Justin Gibson (PwC). These folks have been tremendous to work with and are upping the ante for the quality of our educational events. As always, if you are interested in joining our volunteer team or if you have any questions about or suggestions for the education committee, please do not hesitate to contact me at [shudoba@deloitte.com](mailto:shudoba@deloitte.com).

## COMMUNICATIONS COMMITTEE

---



Justin Gibson  
Committee Chairperson

First off I would like to thank everyone who has helped put this Newsletter together. It was a terrific effort on everyone's part. With the help of the Board of Directors I have been able to put together a wonderful team to help bring consistent, quality information to the Chapter. The new Communications Committee members are Aron Thomas, Dave Lufkin, Sagar Sampat and Meenakshi Lalla.

The Communications Committee has two primary focuses. The first is the Newsletter publication and the second is the Chapter Web site. Our goals for the Newsletter are the publication of four newsletters over the course of the year, two of these will be published in hardcopy format and mailed to you, while all four will be made available in PDF format on the Chapter Web site.

Our goals for the Web site are to execute timely updates on the Web site and in the near future to perform a full review of the entire Web site for accuracy, timeliness, appropriateness, and other areas for improvement.

We are very fortunate to have Allison Leeds our Newsletter Publisher/Designer back with us. Allison was instrumental in

making this an award-winning Newsletter and her expertise is greatly appreciated.

I would like to encourage anyone interested in submitting a technical article for publication in our Newsletter to please do so. If your article is published in the newsletter you will receive \$50.00 per published technical article.

Lastly I would like to invite anyone interested in serving on the Communications Committee to please let me or one of the other Communication Committee members know. There are opportunities to be involved with the Newsletter or the Web site. We are looking for individuals to help with coordination and content, especially anyone interested in sharing your expertise in Web site design.

If you have any comments or suggestions or if you are interested in serving on the Communications Committee please feel free to let me know at [justin.gibson@us.pwcglobal.com](mailto:justin.gibson@us.pwcglobal.com).

## ACADEMIC RELATIONS

Brian Alfaro  
Committee Chairperson

Developing this aspect of SF ISACA (the Chapter) has proven to be an essential component in achieving Chapter goals. The past efforts of Sumit Kalra, Karina Daza, and Jonathon Suryadi have been tremendous contributions to the Chapter, as alumni of San Francisco State University. Edmund Lam and Lance Turcato have also contributed immensely to the well being of students and their career development. Furthermore, many board members have contributed to Student Chapter events as guest speakers to help their organization be a success with quality presentations.

For the coming year the Academic Relations is looking forward toward continuing to remain a strong influence on the Student Chapter. Academic Relations plans to do this by having:

### Internship Programs

This year we plan on helping interested students in finding internships by bridging the gap between the academic arena and the professional world. Academic Relations plans to ask for the support from the Chapter's current members and Board of Directors to provide intern positions at their respective workplaces for these prospective students. Exposure at these internships will be the foundation for students with the desire to pursue careers in IS audit.

### Increased Student Attendance at the CISA Review and Exam

With the current business major emphasis in IT Audit available at SFSU and now at San Jose State University, attendance of the students increased to approximately one third of the review class at the past CISA Review Course. To promote this profession one of the priorities of the Chapter is to continue to increase the number of student attendance in taking the exam and at the Review Course. Further student encouragement can go beyond taking the CISA Exam, to getting involved with Chapter events.

### Professional Chapter Involvement to Support the Student Chapter

As stated earlier, our presence at the university level is very important not only for the students, but for the professional Chapter as well. It is from these events and our encouragement where we find the next generation of members to continue to push toward achieving Chapter goals. As a resource that the student chapter can use, the parent chapter will provide professional speakers, as the Student Chapter sees necessary, to help develop student careers and professionalism.

## RECOMMENDED WEB SITES

Dave Lufkin  
Communication Committee Member

This quarter's featured Web sites are listed below. Access these and other sites from our Chapter Web site at:  
<http://www.sfisaca.org/resources/index.htm>.

### Latest virus information

<http://www.antivirus.com/vinfo/> – Very useful information from Trend Micro on the latest virus information.

### OCC regulations

<http://www.occ.treas.gov/law.htm> – OCC Regulations Web site.

### Symantec

<http://service2.symantec.com/SUPPORT/ent-security.nsf/docid/2001052909504748> – Symantec's site to communicate when their products will hit the end of the support cycle.

### InfoSecurity Online

<http://www.scmagazine.com/scmagazine/thismonth.html> – Info Security Online Articles, an extensive archive of Info Security Online's Web-based articles, dating back to August of 1997.

### IT audit information

<http://www.itaudit.org/> – Provides a fresh perspective on many areas of technology risk, including an IT Audit Forum, online references, guidance for new IT auditors, and an abundance of other useful IT Audit information.

### Dictionary and search engine

<http://www.webopedia.com/> – Advertised as the only online dictionary and search engine you need for computer and internet technology.

### 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.

### 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](http://www.sfisaca.org) to update your contact information.

### ISACA international

(847) 253-1545 voice  
(847) 253-1443 fax  
[www.isaca.org](http://www.isaca.org)

[membership@isaca.org](mailto:membership@isaca.org)  
[certification@isaca.org](mailto:certification@isaca.org)  
[education@isaca.org](mailto:education@isaca.org)  
[bookstore@isaca.org](mailto:bookstore@isaca.org)  
[conference@isaca.org](mailto:conference@isaca.org)  
[research@isaca.org](mailto:research@isaca.org)  
[marketing@isaca.org](mailto:marketing@isaca.org)

### CISA item writing program

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 participating in the CISA Item Writing Program, please request information about the program from ISACA International, Certification Department ([certification@isaca.org](mailto:certification@isaca.org)).

### Contribute to this newsletter

To submit an article or to contribute other items of interest for inclusion in future newsletters, please contact our Communications Committee Chair, Justin Gibson at 415-498-7492, [justin.gibson@us.pwcglobal.com](mailto:justin.gibson@us.pwcglobal.com).



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

# CISA REVIEW COMMITTEE

---



Karina Daza  
CISA Review Chair

## San Francisco CISA Review Course

Over 30 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 that volunteered: Dianna McIntosh from Ernst & Young, Edmund Lam from San Francisco State University, Justin Gibson from PricewaterhouseCoopers, Todd Weinman from Lander International, Sumit Kalra from Charles Schwab, and Vern Thomas from PricewaterhouseCoopers.

## CISA Examination

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

## Ernst & Young Sponsorship

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

## CISA Coordination Committee

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: [karina.daza@ey.com](mailto:karina.daza@ey.com).





## WELCOME TO THE NEW 2001-2002 ISACA BOARD!

Pictured from left to right: Hector Massa, Rick Beckman, Steven Hudoba, Todd Weinman, Bill Davidson, Justin Gibson, Sumit Kalra, Edmund Lam, Christina Cheng, and Stuart White.

Not pictured: Kathleen Arnold and Beverly Davis.

# SAN FRANCISCO CHAPTER BOARD ROSTER 2001/2002

## Executive Board

### President

Todd Weinman  
Lander International  
510-232-4264, ext. 17  
todd\_weinman@yahoo.com

### 1st Vice President

Justin Gibson  
PricewaterhouseCoopers LLP  
415-498-7492  
justin.gibson@us.pwcglobal.com

### 2nd Vice President

Steven J. Hudoba  
Deloitte & Touche  
510-287-2746  
shudoba@deloitte.com

### Treasurer

Christina Cheng  
Safeway, Inc.  
925-467-3563  
christina.cheng@safeway.com

### Secretary

Bill Davidson  
Bay Area Rapid Transit – IAD  
510-464-6954  
wdavids@bart.gov

## Directors

### Directors

Rick Beckman  
Bank of America  
925-675-5282  
rick.beckman@bankofamerica.com

Edmund Lam  
925-830-1234  
edmundlam@onebox.com

Sumit Kalra  
Charles Schwab  
415-636-7686  
sumit.kalra@schwab.com

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

Kathleen Arnold  
Sun Microsystems, Inc.  
650-336-0028  
kathleen.arnold@sun.com

Beverly Davis  
Federal Home Loan Bank  
415-616-2766  
beverlydavis@sprintmail.com

Stuart R. White  
Visa International  
650-432-4320  
srwhite@visa.com

## Committees

### CACS 2002

Beverly Davis, Chair  
Kathleen Arnold  
Steven Hudoba  
Marcus Jung  
Edmund Lam  
Eva Paiva  
Mark Valade  
Todd Weinman

### CISA Review

Sumit Kalra, Chair

### Communications

Justin Gibson, Chair  
Brian Alfaro  
Steven Hudoba  
Sumit Kalra  
Meenakshi Lalla  
David Lufkin  
Sagar Sampat  
Aron Thomas  
Lance Turcato  
Todd Weinman

### Education

Steven Hudoba, Chair  
Rick Beckman  
Deb Frazer  
Mary Laude  
William Luk  
Todd Weinman  
Stuart White

### Membership

Hector Massa, Chair  
Jonathan Suryardi

## Advisory Board

### Advisory Board

Robert Abbott  
Arnold Dito  
Kathryn Dodds  
Chuck Dormann  
Doug Feil  
Carol Hopkins  
Roberta Hunter  
Marcus Jung  
Susan Snell  
Lance Turcato



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