Information Systems Audit and Control Association

SAN FRANCISCO CHAPTER LOCAL AREA NETWORK

FOURTH QUARTER 2002

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

PRESIDENT'S MESSAGE

Beverly G. Davis
President

Contents

President's message....1-2
Calendar of upcoming events 2
SF ISACA luncheon and program....3
Hardening the Unix system III 4-5
Membership....6
CISAReview 2002 7
Announcements....8
CISM 9
CGIinput handling with Perl 10
SF ISACA luncheon and program....11
Sarbanes-Oxley act of 2002....12
President's council meeting....13
Photographs 14-15

A Very Special Thank You!

My gratitude and appreciation is extended to the chapter leaders who presented to our membership an outstanding 2002 eXciting Fall Conference. It gives me great pleasure to acknowledge on behalf of the Board of Directors how grateful we are to have such commitment to excellence and we would like to say thank you for all of your dedication and hard work. Special acknowledgements are extended to the following individuals:

Todd Weinman, Past President, provided the framework for this year's conference and his involvement was extremely valuable. His leadership to the Education Committee gave us the direction, support, and the driving force to deliver yet another successful three-day training event.

Gloria Lievano, 2nd Vice President and Education Committee Chair accepted the challenge to take on the responsibility as committee chair and delivered a program of exceptional session speakers. The background work of coordinating and scheduling the speakers was superbly managed.

Lisa Corpuz, Secretary was the behind the scenes facility manager. This year's logistics were seamless and all of the coordination, planning, and delivery are attributed to Lisa's organization and follow-through.

Anne Woodbury, Treasurer assisted with the registration and served as a session proctor. The mere fact of having someone you can count on to fill-in when needed was the support Anne gave to the conference.

Special thanks to those committee members who served as session proctors:

- Christina Cheng
- Bill Davidson
- Dave Lufkin
- Jennifer Smith

A very special thanks to the Education Committee members who helped implement this year's conference program strategy. Acknowledgements are extended to:

- Carey Carpenter
- Helen Leung
- Maryam Malek
- Cliff Nalls
- Roy Vaiani

Last but not least is the Lander International staff, specifically Helen Winters and Tim Sawyer, who assisted with the marketing and conference registrations. Without Lander's support staff, many of the chapter's education events would not have materialized.

PricewaterhouseCoopers, Deloitte & Touche, KPMG, PentaSafe, and Lander International supported this year's conference sponsorship. We welcome your support, thank you for your generosity, and we are hopeful that your companies will continue to support our chapter events.

As we look forward to completing this year's education calendar we will have the opportunity to work with yet another strong leader, Gloria Lievano. This is a leadership change for the Education Committee. Thank you Gloria for accepting the Chair position, we are behind you, and you can expect a 100% support from the Board and

PRESIDENT'S MESSAGE – continued

your committee. We are grateful that you have accepted this role and the challenge of providing quality education events to our members.

Many of you are unaware of the many tasks and countless hours it takes to plan the chapter's education events. To no avail we have been fortunate to have the knowledge and support of Todd Weinman. His contributions have been above and beyond the call of duty and it is a great feeling to know that he is still behind the scenes making things happen.

The San Francisco Chapter of ISACA is committed to providing the membership with quality education events and we are proud to say that we have a team of dynamic individuals. The upcoming educational events are in the planning stages and we are always in need of volunteers. If you are willing to give of your time or talents, please e-mail me at davisb@fhlbsf.com. We welcome your participation!

A very special thanks to the Education Committee and the leaders who delivered an exceptional 2002 eXciting Fall Conference!

Sincerely,

Beverly G. Davis
President

CALENDAR OF UPCOMING EVENTS

Date	Event	Place	More information
November 20, 2002	SF ISACA Full Day Seminar	Bank of America Data Center, 1455 Market Street, San Francisco	http://www.sfisaca.org/events/2002-November.htm
December 19, 2002	SF ISACA Luncheon Presentation	The Palace Hotel, San Francisco	http://www.sfisaca.org/events/2002-December.htm
January 16, 2003	SF ISACA Full Day Seminar	The Palace Hotel, San Francisco	details to be posted at www.sfisaca.org
February, 2003	SF ISACA Luncheon Presentation	The Palace Hotel, San Francisco	details to be posted at www.sfisaca.org
March, 2003	SF ISACA Full Day Seminar	The Palace Hotel, San Francisco	details to be posted at www.sfisaca.org
October, 2003	SF ISACA 3-Day Fall eXciting Seminar	TBD	details to be posted at www.sfisaca.org
National events			
May 18-22, 2003	North American CACS	Houston, Texas	http://www.isaca.org/nacacs2003.htm

SF ISACA LUNCHEON AND PROGRAM

Security Management by the Numbers: Benchmarking Your Processes and Practices with the Security Management Index • Thursday, December 19, 2002 • 1.5 hours of CPE credit

Session description

Todd will present an overview of The Security Management Index and how security managers can begin to benchmark their company's security management practices.

The Security Management Index at www.humanfirewall.org is a free online survey that is based on the 10 major areas of ISO17799. Security professionals are taken through a series of questions regarding their security management practices and receive results in the form of a score. This score tells them how they are doing against ISO standards and offers a comparison of their security management practices with others in their industry. Aggregate data from the survey will be used to compile a global Security Management Index Report that will help security professionals identify trends and establish metrics for security management as an ongoing, strategic business function.

In this session, security professionals will learn about:

- Using ISO to measure security management practices.
- Best practices in security management.
- Benchmarking methods for comparing security management best practices with other organizations by industry and peer group.
- How to raise security awareness among upper management executives, helping explain and justify improving security measures and budget.

Speaker bio

Todd Tucker is the Director of Security Architecture & Strategy for PentaSafe Security Technologies. Todd is a security subject matter expert responsible for understanding the needs and challenges of PentaSafe's clients and the information security market. Todd works directly with clients, industry analysts, partners and others to develop the product strategy, generate product requirements, and offer other ideas to enhance the value of PentaSafe's offerings to the market. Prior to joining PentaSafe, Todd was the Senior Director of Industry Solutions for e-Security, Inc. Todd was responsible for developing solutions based upon e-Security's products to meet the needs of e-Security's largest target segments. Todd developed the industry solutions approach in order to target financial services, telecommunications, government, healthcare, and managed service providers.

Register

To register or to find other important details about the program, visit our Web site: www.sfisaca.org

Schedule

Time	Description	Pricing (including Saver Pass info (if applicable)
11:30 am - 12:00 noon	Registration	$40 Members (or 1 Saver Pass)
11:30 am - 12:30 pm	Lunch	$50 Non-members (or 1 Saver Pass plus $10)
12:30 pm - 2:00 pm	Presentation	$20 Students
		Payable in cash, check, or Saver Pass only – no credit cards.

Location

The Palace Hotel, in San Francisco's Financial District at the corner of Market and New Montgomery Streets
2 New Montgomery Street, San Francisco, CA 94105, 415-243-8062

Cancellation Policy

If after submitting your reservation you determine that you need to cancel, please do so at least 72 hours prior to the event by contacting the registration coordinator, Tim Sauer, at either tim@landerint.com or at 510-232-4264 x24.

Please do not be a 'no show'. Our Chapter is billed for reservations made with our facilities provider, and we will have to pass the charges on to you. Thank you for your cooperation.

HARDENING THE UNIX SYSTEM, PART THREE

PART THREE

by Dan Hilton
Audit Consultant
Bank of America

In the 2nd and 3rd quarter newsletters, Part One and Part Two of *Hardening the Unix System* was presented. The purpose of this three-part article is to introduce steps an auditor can take to help ensure the Unix system is properly configured.

Strengthening the controls associated with a Unix environment is crucial to many organizations because these systems may host critical business applications. If not properly secured, the security and reputation risks can be significant. Part One and Part Two of this article spoke of rhost files, netrc files, the host.equiv file, login banners, password settings, umask settings, user ids, system services, and system timeout.

Part Three, the final segment of this article, will discuss three other areas that should be considered during a comprehensive Unix review: miscellaneous file review, security patch procedures, and password cracking.

Miscellaneous file review

Description

The Unix file is a labyrinth of hierarchical design. Starting from the root level directory, thousands of additional directories and files can be setup to support applications, system utilities, and users. Often times, users will create files and directories with good intention of supporting the system, but sometimes these files will store information that can be used to exploit a system.

Control

A hypothetical scenario may include the following: A system administrator may conduct a periodic review of password strength on a system. To conduct this review, the administrator may copy the shadow file (see Part One of this article) so a password-cracking tool can be run against the file. Following the review, the non-compliant users are identified and the administrator is done. However, the administrator may neglect to remove the copy of the shadow file and it could be left readable by all users with access to the system. A user can then copy this file and use it to decrypt passwords that can be used to exploit the system.

Files such as the ones mentioned in the scenario above should not exist on the system. When a Unix audit is conducted, the auditor should review various system directories and files for this level of information. If the auditor is experienced in navigating the system, they should request access to review various file systems, or they should sit with a system administrator to review the necessary files.

File(s) to review

This is not a simple review to conduct, and can take a significant amount of time. However, there is a method that can be used to help reduce the amount of time it takes to review the system. First, the user can use the list command to navigate the system and review various high-level directories. For example, the following command will list the root directory:

```
ls -al /
```

Once a directory is listed, the auditor can review additional directory names and files that are not standard to the system. For example, the root directory may have a file named .rhostbackup. Often times, this is a backup for the actual root level rhost file and may be identical to the actual file. Some suggested directory names or file names to look for would include anything with passwd, password, admin, administrator, netrc, or root listed in the name. There is a quick way to look for files or directories with these names. The following find command can be executed to check the entire file structure for this type of information.

```
find / -name [insert key word] >> [file
name to store information]
```

An example of this command would read in the following manner:

```
Find / -name passwd >> password named
files
```

The output of this command will be placed in the directory that the user currently resides when the command is executed. The results of the review will not ensure that all unsecure files will be found, but it will definitely help reduce or remove some files that can be used to exploit the system.

Security patch procedures

Description

As stated multiple times, there are constantly new vulnerabilities that are found for every type of Unix system. When these vulnerabilities are identified, the producer of the operating system (i.e. Sun Microsystems, IBM, or HP) will develop a patch to ensure the vulnerability can be appropriately addressed. While the patch is created and made available, it is the responsibility of each organization to ensure the patches are applied to their systems in a timely manner.

Control

Unix system producers typically have a method of communicating the release of a patch to the general public and customers. An organization should have a process in place that ensures these communications are reviewed, each vulnerability is fully analyzed, and based upon that analysis, the appropriate patches are installed.

File(s) to review

An auditor should interview the system administrator to fully understand the process that is used to become aware of new patches and to install these patches on each system.

Security Focus (www.securityfocus.com) developed a tool called the Solaris Vulnerability calculator. A command can be run against a Solaris system that will give an output of patches that need to be installed on the particular version of the system being analyzed. The command is the following:

```
showrev -p | cut -f2 -d' '| xargs >>
[file name to store information]
```

The output of this command can be input into the vulnerability calculator. The calculator will then give an output stating the vulnerability that each patch was designed to fix.

Password cracking

Description

As discussed in Part One of this article, a user or system password is crucial to the security of the system, and there are many settings that must be set to ensure adequate passwords are being used on the system. There is one other method to ensure passwords are adequate, and that is the use of a password-cracking tool. There are multiple password-cracking tools that are available and can be used to check password compliance.

Control

Contingent upon company policies, an organization should consider the periodic use of password cracking tools to ensure all users are complying with company password baselines. If such tools are used, a detailed set of procedures should exist governing the method of how these tools are used and stating who has the right to use such tools.

File(s) to review

An auditor should first document the process that is used by the organization to validate password compliance. The process used by a particular department should be well documented and understood by all. In addition, some organizations permit the audit department to validate compliance with password standards by using password-cracking tools. If this is allowed, there are several tools available that can be used to check passwords. One such tool is called John The Ripper. See the following Web site to read more information about this tool: http://www.openwall.com/john/.

Conclusion

The topics discussed in this three-part article are certainly not all the potential vulnerabilities on a Unix system. New vulnerabilities and security holes are frequently identified which require security patches and new controls. Much like any other technology, you must make an effort to read various periodicals and books that publish new information. The following are a few recommended sources of Unix information:

- Practical Unix & Internet Security, by: Simson Garfinkel and Gene Spafford
- http://www.sans.org/
- http://www.geek-girl.com/unix.html
- http://www.unixreview.com/

There are several audit Web sites that provide various Unix audit programs that differ based upon the type of review that needs to be conducted. Listed below are a few of the Web sites that provide different types of programs and checklists. These are excellent resources when trying to understand all key areas that should be included in a Unix review.

- http://www.auditnet.org/
- http://www.all.net/books/audit/

The purpose of this three-part article was to discuss the various controls in a Unix environment and the risks of not properly implementing these controls. Also, discussed, was the method by which an auditor can review such controls. By reviewing the information provided in this article and using the information provided in the Web sites above, it should improve your understanding of how to help secure a company's Unix systems. The security and reputation risks of not understanding and not auditing the Unix environment can be significant.

MEMBERSHIP

Bill Davidson
Committee Chairperson

The membership count for the San Francisco Chapter as of November 1, 2002, stands at 403 members. Please join me and the San Francisco ISACA Board of Directors in welcoming the following new Chapter members:

Angela M. Basi
Ernst & Young

Shari Bley, CISA, CPA
Legacy Marketing Group

Jay W. Bolton, CISA, CPA
PricewaterhouseCoopers

Lisa M. Brownen
Ernst & Young

Edwin W. Byers, CMA
Deloitte & Touche

Robert L. Grill, CISA, CISSP
Wells Fargo

Bradley D. Hart, CA
Visa International

Vladimir Itskovsky
DigitalVAR, Inc.

Jeremy A. Lapidus, CISA, CIA
University of California, Berkeley

Venetia C. Lau, CPA
Ernst & Young

Daniel F. Lee
San Francisco, CA

Eric C. Longo
KPMG

Tihomir V. Nedkov
Deloitte & Touche LLP

Odabi I. Odabi
County of Alameda

Midori Ohno, CIA
Treasury IG

Andrew L. Qualls
Pleasant Hill, CA

Robert L. Schock, CIA
Federal Reserve Bank of San Francisco

Ella R. Stetser, CISSP
Lucent

Angela M. Stewart
US Department of Labor

Miguel O. Villegas, CISSP
Wells Fargo Bank

CISA REVIEW 2002

Sumit Kalra
former Committee Chairperson

The 2002 CISA review course exhibited yet another success story for the San Francisco ISACA chapter with a 54% passing rate. Congratulations to the following review course attendees for passing the 2002 CISA examination and for ranking in the top three among all San Francisco CISA examination participants:

• Ms. Anna Gennadyevna Tchernina, No. 1 scorer

• Mr. John W. Holmes, CPA, No. 3 scorer

Year after year, the SF chapter has achieved great success in hosting the review course, providing a pool of talented professionals as instructors and motivating the group of students interested in furthering their careers. SF chapter's CISA review course committee was invited to the western region President's Council Meeting in October to share its CISA success story three years in a row.

Special thanks to the following instructors who contributed to the success of the 2002 review course:

Domain	Instructors
The IS Audit Process	Carey Carpenter, Deloitte & Touche and Todd Weinman, Lander International
Management, Planning, and Organization	Sumit Kalra, Charles Schwab
Technical Infrastructure and Operation Practices	Edmund Lam, Professor San Francisco State University
Protection of Information Assets	Joshua Mock, PeopleSoft
Disaster Recovery and Business Continuity	Stuart White, VISA
Business Application System Development, Acquisition, and Maintenance	Douglas Feil, Independent Consultant
Business Process Evaluation and Risk Management	Maria Shaw, Deloitte & Touche

Motivating the students has been a challenge every year during the eight beautiful sunny weekends prior to the exam. This year our motivational approach included providing strong Columbian dark coffee, Krispy Kreme donuts, bagels and most importantly, the 7-minute BMW M3 (www.BMWfilms.com) commercial directed by Guy Richie starring Madonna.

During the last day of the Fall seminar the SF chapter recognized the volunteer instructors for their contributions and the passing students for their hard work. Brian Alfaro of Deloitte & Touche will be chairing the 2003 CISA review course committee. Congratulations to Brian Alfaro as well for successfully passing the CISA examination this year.

At last I would like to thank all the volunteers (San Francisco State University students, review course students and the instructors) for making the SF chapter's review course the best! As for me, I will be spearheading the 2003 Academic Liaison committee to educate the local institutions addition to SF State University the importance of an IS audit career.

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, William Davidson (wdavids@bart.gov), the name, address, phone number, and e-mail 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 wdavids@bart.gov to ensure that you receive important information electronically.

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

ISACA international

847-253-1545 voice
847-253-1443 fax
www.isaca.org

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

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).

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, Christina Cheng at (925) 467-3563, or christina.cheng@safeway.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

CGI INPUT HANDLING WITH PERL

By Bob Grill
Senior IS Auditor,
Wells Fargo

This article discusses some of the differences between the GET and the PUT methods for passing data from HTML forms and how these methods affect CGI input handling in Perl.

Almost every information system auditor is aware that the GET method is not recommended. The primary reasons for not using the GET method are related to privacy issues. When the GET method is used, the input is placed in an environmental variable called QUERY_STRING and appears in the browser address bar after the input is submitted. The browser URL stays in the browser cache by default and these strings might also be logged on the server side. The information contained in the GET request may contain sensitive information.

Another disadvantage of the GET method is the limitation on the amount of data that can be submitted to the CGI script. To see all of your environmental variables including how the Web server sees normal Web page requests, go to http://cpcug.org/scripts/env.cgi. Remember that all the information shown is considered input to any CGI program. It is simple to write your own Perl program to view your environmental variables.

Input checking as related to Internet applications is based on not trusting any client side input (e.g., a user's browser). Input includes not only what is put in form prompts or the address bars, but can include cookies, state maintenance information, environmental variables and layer 3, 4 and 5 packet information. One can see the information being passed to the server from the client at layers 3 through 5 with a tool called TCPDump (http://www.sustworks.com/site/ipmx_tcpdump.html). You could also manipulate this data using a variety of tools. For layer 6 and above, use a tool called Web proxy (http://www.atstake.com/research/tools/index.html). This tool can be used to manipulate the data also.

But what about the PUT method? The PUT method takes your input and stores it in a variable called "standard input" or STDIN. A Perl program then reads this variable and uses it in its CGI script. For example, in your browser's view source window you may see a line like this:

```
<FORM ACTION="GetSTDIN.pl" Method =
"POST">
```

The data entered into your browser is sent to the GetSTDIN.pl program when the submit button is clicked. If the file GetSTDIN.pl has a line that says `read(STDIN, $Stuff_Input);`, the program will place the value of what is submitted from the HTML form into the STDIN variable and label it as $Stuff_Input.

With the exception of the privacy issues, this method has all the same risks as the GET method including cross site scripting, buffer overflows and SQL Injection. Accordingly, this input should not be trusted. A great utility in Perl to help prevent processing malicious data is to end the very first line of every Perl program (called the "Sh-bang line") with a -T. For example, the first line might look like this:

```
/usr/local/bin/perl -T
```

The "-T" flag forces the programmer to use regular expressions to search through and cleanse the data in the $Stuff_Input string placing only the expected data in a new variable, say $Clean_Input. The "-T" flag requires that only the new variable be used to modify files, directories or processes.

Perl runs server side. For a better understanding of Perl and these methods, I recommend downloading Perl from http://www.activestate.com/ for Win32 systems or from www.perl.com for all other distributions. Since Perl is interpreted, you can read the source code in a text editor.

Next quarter's article will be on the dangers of using the strncpy function when programming in C++.

SF ISACA LUNCHEON AND PROGRAM

Network Firewall Security • Thursday, January 16, 2003 • 7.0 hours of CPE credit

Session description

This full day presentation will provide a basis of understanding of what firewalls can and cannot do. It will include a discussion of the operational components of managing firewalls, options for developing an audit program, and ways to ask questions so you can get honest answers and understand the information generated. The presentation will be broken down into the following four main modules.

Module 1: Understanding Firewalls

- Firewall Architecture Overview
- Organizing Network
- Types and Products
- Risk and Difficulties
- Proxies
- E-mail, FTP, Web, SMTP, HTTP

Module 2: Understanding Firewall Operations

- Administration Access
- Authentication
- Monitoring
- Logging
- Break/Fix Response
- Policy Rule Administration
- Blocking Sites/Ports

Module 3: Understanding Firewall Policies

- Mapping Policy to Firewalls
- Policy as the Underpinnings of a Secure Firewall Infrastructure
- IPSec

Module 4: Firewall and Auditing

- Building An Audit Plan
- How To Ensure The Responses Are Factual
- Good Ideas Versus Audit Findings

Speaker bio

Kurt Kruse and Brett Anderson, Wells Fargo. Detail bios to come.

Register

To register or to find other important details about the seminar, visit our chapter Web site: www.sfisaca.org

Schedule

Time	Description	Pricing (including Saver Pass info (if applicable)
8:00 am - 8:30 am	Registration and Breakfast	$110 Members (or 3 Saver Passes)
8:30 am -11:30 am	Morning Session: Network Firewall Security	$135 Non-members (or 4 Saver Passes)
11:30 am -1:00 pm	Lunch	$75 Students
1:00 pm - 4:30 pm	Afternoon Session: Network Firewall Security	Payable in cash, check, or Saver Pass only – no credit cards.

Location

The Palace Hotel, in San Francisco's Financial District at the corner of Market and New Montgomery Streets
2 New Montgomery Street, San Francisco, CA 94105, 415-243-8062

Cancellation Policy

If after submitting your reservation you determine that you need to cancel, please do so at least 72 hours prior to the event by contacting the registration coordinator, Tim Sauer, at either tim@landerint.com or at 510-232-4264 x24.

Please do not be a 'no show'. Our Chapter is billed for reservations made with our facilities provider, and we will have to pass the charges on to you. Thank you for your cooperation.

SARBANES-OXLEY ACT OF 2002: THINGS YOU SHOULD KNOW

By Christopher Mak
Senior Manager of the
Enterprise Risk Services Group,
Deloitte & Touche

IS Auditors and Internal Auditors alike face a lot of new, post-Enron challenges as they have never before. The press would lead you to believe that this could be the year of the internal controls auditor. In response to popular support for a war against America's evil corporate ethics and irresponsibility, this summer Congress passed a bill known as the Sarbanes - Oxley Act of 2002. As a result of this Act, series of regulations will impact the future of the auditing profession.

For SEC Registrants, the impact of Sarbanes-Oxley is no longer confined to the accounting department, but defines specific responsibilities onto the CEO and CFO of these registrants to perform certain actions. In summary, they include:

- Perform an evaluation as to the quality of the system of internal controls, specifically those internal controls which protect the reliability of disclosures made to the investing public (including 10-K (annual) and 10-Q (quarterly) financial statements and associated management discussion and analysis.
- Certify publicly that the systems were reliable in each quarterly filing.
- Report any instances of fraud (however significant or insignificant) performed by the people involved in financial reporting to the audit committee and auditors.
- Report any significant failures of the internal control systems to the audit committee and auditors.

One thing that should be noted is that the full implementation of the Sarbanes-Oxley Act of 2002 has not yet occurred. Future rules anticipated in 2003 will require an independent accountant attestation for a "report on internal controls" (another management responsibility to be defined by Sarbanes-Oxley).

In the short term, the IS Auditor, whether part of a public accounting firm, or in industry, should be alert to opportunities to:

- Help CEOs and CFOs to understanding what their certifications mean - specifically what are the risks that internal controls are not effective? What areas should be evaluated?
- Make an assessment of work already done to help evaluate controls.
- Create a culture of understanding in respect of internal controls in both the company's financial systems and information systems infrastructure.
- Communicate about the importance of reliable IT controls in internal controls processes, and more aggressively pursue correcting prior issues.
- Be the bridge between the internal audit, financial reporting, information technology functions, and the external auditors.

WESTERN REGION PRESIDENT'S COUNCIL MEETING

Over the weekend of October 5 & 6, our Chapter President and three of our Board members attended the annual western region President's Council Meeting (PCM) in Albuquerque, NM. The PCM, hosted this year by the New Mexico Chapter, provided a forum for sharing ideas on how to better run our Chapters. It was an excellent way to find out what other chapters in the western region are doing and to bring back some good ideas. We also had a chance to develop networking contacts with other chapter leaders and to develop our leadership.

– William Davidson

Attending a President Council Meeting (PCM) was a great experience. The experience of sharing accomplishments and ideas with colleagues throughout the western region was extremely beneficial. Just knowing that other leaders are having similar issues and finding ways to address those issues made the time spent well worth it.

What I found valuable was the exchange of information from trusted sources that provided tested results. It was most rewarding to gain a new knowledge base from my peers of extremely experienced individuals. Their willingness to share and critique has added value for me personally and professionally. Thanks for the candidness and I enjoyed exchanging ideas with Western Region Leadership group.

– Beverly G. Davis

The Western Region President Council Meeting held on October 5 & 6 at Albuquerque, New Mexico was an informative, fun-filled and inspiring conference. It provided a great opportunity to meet and network with the other chapter leaders. It also served to exchange new ideas and to validate our chapter's practices.

Beverly Davis, our Chapter President discussed our Chapter's officers/incorporation insurance program and led a team building exercise with the group while Sumit Kalra, our CISA Review Chair, shared the success of our CISA Review program. Lynnea J. Banach from ISACA International enlightened us with a body of information about services and resources that are available for local chapters such as the Marketing Fund program. Other topics such as Chapter Newsletter, Chapter Web site and Life After Local Chapter Involvement were also presented. I left the conference feeling motivated by the energy and commitment displayed by the chapter leaders. I would like to thank the Chapter for the opportunity to share such a memorable experience.

– Christina Cheng

The 2002 Western Region PCM was a very enlightening experience for me. Because I am a fairly new member to ISACA as well as a new board member to the chapter, the conference was a great way to learn about ISACA and to learn what other chapters are doing for their chapter members. The highlight of the conference was meeting other chapter leaders and seeing the dedication and commitment that these leaders have towards providing quality service to their members. There was a lot sharing of ideas and a great deal of support for one another. I think that everyone that attended the conference came away with a positive outcome and with many new friends.

– Lisa Corpuz

Front row from left to right: Aleksandra Looho (LA Chapter), Bill Hossley (New Mexico Chapter), Thomas Phelps (LA Chapter), Harriet Thiesen (Denver Chapter), Nancy Winston (Willamette Valley Chapter).

Back row from left to right: Cheryl Santos (LA Chapter), Edward Paz (New Mexico Chapter), Lisa Corpuz (SF Chapter), Christina Cheng (SF Chapter), Beverly Davis (SF Chapter), Sumit Kalra (SF Chapter), Sudha Chadalavada (Silicon Valley Chapter), Bill Davidson (SF Chapter).

Left to right: Greg Ash (LA Chapter), Thomas Phelps (LA Chapter), Christina Cheng (SF Chapter), Lisa Corpuz (SF Chapter).

Front row left to right: Lisa Corpuz, Christina Cheng, Sumit Kalra (all from San Francisco Chapter)

Back row left to right: Harriet Thiesen (Denver Chapter), Lynnea Banach (International), Alan Bajkov's wife, Alan Bajkow (Vancouver Chapter), Edson Gin (LA Chapter), Cheryl Santor (LA Chapter), Bill Davidson (SF Chapter), Charles Dormann (International), Anita Montgomery (LA Chapter), Steve Thorsted (Utah Chapter), Michael Pach (Sacramento Chapter).

SAN FRANCISCO CHAPTER BOARD ROSTER 2002/2003

Executive Board

President
Beverly Davis
Federal Home Loan Bank
415-616-2766
davisb@fhlbsf.com

1st Vice President
Christina Cheng
Safeway, Inc.
925-467-3563
christina.cheng@safeway.com

2nd Vice President
Gloria Lievano
Pacific Exchange
415-393-7933
glievano@pacificex.com

Treasurer
Anne Woodbury
Providian Financial
925-738-4849
anne_woodbury@providian.com

Secretary
Lisa Corpuz
Providian Financial
415-278-8713
lisa_corpuz@providian.com

Directors

Directors
Brian Alfaro
Andersen LLP
415-546-8200
balfaro@deloitte.com

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

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

Carey Carpenter
Deloitte & Touche
415-783-5290
ccarpenter@deloitte.com

Dave Lufkin
Bank of America
925-675-1878
dave.m.lufkin@bankofamerica.com

Jennifer Smith
Wells Fargo
415-396-7955
smithjen@wellsfargo.com

Todd Weinman, past president
Lander International
510-232-4264, ext. 17
todd@landerint.com

Committees

Academic Relations
Sumit Kalra, Chair

CISA Review
Brian Alfaro, Chair
Sumit Kalra
Helen Sun

Communications
Christina Cheng, Chair
Lance Turcato, Web Master
Brian Alfaro
Doug Feil
Robert Grill
David Lufkin
Maria Shaw
Aron Thomas

Membership
Bill Davidson, Chair
Hector Massa

Education
Gloria Lievano, Co-chair
Todd Weinman, Co-chair
Carey Carpenter
Lisa Corpuz
Jim Kastle
Helen Leung
Gloria Lievano
William Luk
Maryam Malek
Cliff Nalls
Jennifer Smith
Roy Vaiani
Stuart White

Volunteer
Todd Weinman
Helen Sun, at large volunteer

Advisory Board

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

Information Systems Audit and Control Association

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