Information Systems Audit and Control Association

SAN FRANCISCO CHAPTER LOCAL AREA NETWORK

SECOND 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

Todd Weinman
President

Welcome to our final newsletter of the 2001-2002 Chapter year and my last as President of the San Francisco Chapter. I am grateful for the opportunity to have served as your President over the past year and to have had the opportunity to work so closely with the many outstanding individuals on our Board of Directors and volunteer committees. It was the combined efforts of all of these people who enabled us to accomplish one of our most successful years ever. The following are just a few of the highlights of how your Board and volunteers have added value to the membership over this past year:

- Hosted our first three-day multi-track seminar in September 2001.
- Increased the number and variety of education offerings, combining the Fall Seminar with several full day seminars and luncheon presentations.
- Significantly increased the level of technical content of our newsletter.
- Successfully hosted the North American CACS conference in May 2002.
- Continued to set examples for other chapters with our award-winning Web site.
- Improved our budgeting process to better account for the optimal use of Chapter funds.

Throughout the year we were able to overcome a number of challenges. One of those challenges consisted of hosting our first ever Fall Seminar just a week and a half after the events of 9/11, and with several of our speakers flying in from other parts of the country. Another challenge was faced when our 1st and 2nd VPs, **Justin Gibson** and **Steven Hudoba**, who were also our Communication and Education Chairs respectively, both relocated out of the Bay Area within a month's time. The faulty systems conversion of our former Web host ended up freezing our Web site for several weeks in the fall and necessitated our own speedy conversion to a new host. And there were other smaller hurdles such as the inevitable last minute speaker cancellation (always a personal favorite). But in every instance, because of the strong contributions of our volunteers, we were able to overcome these obstacles.

In the following paragraphs, I'd like to give acknowledgement to some of the key contributors from this past year. While space constraints prohibit recognition of all of those who volunteer (a list of our chapter committees can be found on the back page of this newsletter), the following are some of our most notable contributors. Recognition of those companies that gave strong support to the Chapter can be found on page 10 of this newsletter in the article, *Corporate Superstars*.

Certainly, the success of this past year could not have been accomplished without the strong efforts of the previously mentioned Gibson and Hudoba. Justin, Steven and I engaged in weekly meetings months before the Chapter year actually started in order to set the blue print for the year. Steven's strong leadership of the Education Committee and contributions to improving our budgeting process were particularly notable. His commitment and leadership set a strong example for all to follow.

Similar credit must be given to the whole Education Committee. **Rick Beckman** provided strong leadership of the Committee after Steven's departure. He also helped arrange for our Full Day Seminar that was held at Bank of America facilities in

Contents

PRESIDENT'S MESSAGE – continued

November, presented at our October luncheon and helped facilitate our April seminar. The Education Committee is the most challenging of all of the committees, so I'd like to recognize our other Education Committee contributors: **Stuart White**, **Deb Frazer**, **William Luk**, **Mary Laude**, **Lisa Corpuz**, **Carey Carpenter**, **Anne Cole** and **Jim Kastle**.

Special acknowledgement should also be made to our CACS team led by our incoming President, **Beverly Davis**. As a chapter President, one always has an appreciation for the things that you don't have to worry about. With Beverly leading the CACS committee, I could confidently focus my attention on other areas. **Marc Jung** did a fine job of coordinating our CACS volunteers, and acknowledgement should also be made to **Kathleen Arnold** and especially **Gloria Lievano** who put together our visitor guide.

Dave Lufkin of our Communications Committee also deserves recognition. Not only was he the source of a great deal of our increased technical content for the newsletter, but he also played a key role in organizing our Full Day Seminar at Bank of America.

Christina Cheng was vital in revamping our budgeting process as we went into the Chapter year. She has now taken leadership of the Communications Committee, including overseeing production of this newsletter. I also appreciate the way in which Christina and **Anne Woodbury** worked together to make for a seamless transition of our Treasurer position.

Sumit Kalra did a fine job of organizing and running our CISA Review Course, including teaching one of the sessions.

Former President and Webmaster **Lance Turcato** receives special recognition as well. Not only did he oversee the migration of our Web site to a new host, and in the process redesign the whole site, but also he carried out Web duties for much of the year without a backup. Lance's work on the Web site was recently recognized by International with a Silver Level Web site award.

Hector Massa and **Bill Davidson** and **Brian Alfaro** contributed with solid consistent efforts as Membership Chair, Secretary and Academic Relations Chair, respectively.

Moving Forward

As we look ahead to next year, I am confident that we will continue to improve on this year's accomplishments. I take great comfort in leaving the Presidency in the very capable hands of **Beverly Davis**. Of course as I learned this year, the President is only as strong as the volunteers that support him/her. Consequently, I encourage each of you to consider the rewarding experience of volunteering for your local Chapter.

Warmest regards,

Todd Weinman

CALENDAR OF UPCOMING EVENTS

Date	Event	Place	More information
July 18, 2002	SF ISACA Luncheon Presentation	The Palace Hotel, San Francisco	details to be posted at www.sfisaca.org
September, 2002	SF ISACA Luncheon Presentation	The Palace Hotel, San Francisco	details to be posted at www.sfisaca.org
October 9-11, 2002	SF ISACA Fall Seminar	The Palace Hotel, San Francisco	details to be posted at www.sfisaca.org
November, 2002	SF ISACA Full Day Seminar	TBD, San Francisco	details to be posted at www.sfisaca.org
December, 2002	SF ISACA Luncheon Presentation	The Palace Hotel, San Francisco	details to be posted at www.sfisaca.org
International events			
July 7-10, 2002	ISACA International Conference	Mariott Marquis, New York	http://www.isaca.org/international2002.htm
August 12-14, 2002	ISACA Network Security Conference	Ceasars Palace, Las Vegas	http://www.isaca.org/international2002.htm

AUDITING USING SCRIPTS by Robert Grill

The independence required by an auditor makes it difficult to perform technology audits. To get the information that an auditor needs to perform technology audits requires administrative (super user) access to the system being audited. This can jeopardize the auditor's independence and expose the auditor to blame for production problems. Accordingly, to audit the system, the auditor requires a tool that assumes administrative privilege to read and report on information without the ability to alter the system configuration. Often this requires software to be loaded on the system to be audited. Many vendors sell tools that perform this function; below are some examples.

Operating System	Vendor Tool Manufacturer
OS/400	PentaSafe
Windows, Novell, UNIX	Bindview, Axent
OS/390	Consul

All operating systems have scripting languages that could be used to create audit tools. UNIX does not have to provide interfaces because it is file and text based. However, Windows gets more complicated because of the registry and active directory databases. Developers of Windows scripts can use Active Directory Service Interfaces (ADSI) to facilitate writing scripts that query information from these database constructs.

The more popular scripting languages are Java Script, Visual Basic Script, Perl and Rexx. Executable commands available at the operating system's command line can also be concatenated into audit tools by the use of scripts. These are often called batch files or shell scripts.

Once these scripts are written the auditor requires the software to be loaded locally on the system where the information is stored. The script must be run by a user with administrative privileges. Also, the information gathered by these scripts requires removable media or a network connection to move the information to the auditor's machine for further analysis. A sample of a UNIX audit script can be viewed at http://www.giac.org/practical/Robert_Grill_GCUX.doc (Appendix B). A script can be run over the network, but the effort involved in configuration changes is not worth the benefit.

The main advantage of writing a script instead of using a tool is cost. The cost of a script is free and can usually be found and downloaded from the Internet. Auditors can also write the scripts, and with practice, auditors will prefer these to tools because of the customization opportunities and convenience. Purchased tools and scripts require software to be loaded on the system where the information is stored.

An administrator who is accountable for the availability of the machine is more likely to welcome a script than a third party tool. Administrators use scripts on a daily basis to perform their jobs. Supplying administrators with a script is preferred by them because they can become comfortable with it by reviewing the code. Without the copyright burdens associated with a tool the administrator can keep the script as a benefit from the audit.

Scripts can be run without the administrator by configuring the script to run as another user. This would eliminate not only the risk that the administrator might change the information before the script results are given to the auditor, but also the awkwardness of looking over the administrator's shoulder when running the script. However, in this auditor's opinion, the cost of the script running as another user is not worth the benefit.

In summary, scripts:

- Reduce costs
- Add freedom and flexibility to auditors in performing their duties
- Administrators prefer scripts to third party tools because they can review the source code before it is loaded on the system

Scripts offer more advantages than disadvantages over tools for the auditor who invests the time to learn how to write them.

About the author
Robert Grill is an IT Audit (Systems) Project leader at California Federal Bank. He has a BS in Accounting, and an MBA with a concentration in Management Information Systems. He is a CISA and a CISSP. Bob is a contributor and grader for the SANS GIAC Systems and the Network Auditor (GSNA) certification program.

VENDOR SYSTEMS DEVELOPMENT LIFE CYCLE by Douglas Feil, CISA

The traditional Systems Development Life Cycle approach has been in use for developing new application systems in many organizations throughout the world. The SDLC methodology sets a standard for the organization for the planning, execution, and implementation for a new systems project. However, the current trend is for organizations to buy versus build their application specific systems. This purchase option creates the need for a new approach by the IS Auditor to assure that the appropriate controls are available in the acquisition of a Vendor application system.

The intent of this article is to identify areas in the vendor systems acquisition process where the IS Auditor can add value to an important organization business initiative. This article is based on the author's experience in working as an IS Auditor on a variety of application systems development projects and the selection of vendor solutions for a variety of business organizations.

The content of this article is presented in a manner to be most useful by all levels of IS Auditors. Each new acquisition project will vary in approach and complexity among organizations. Therefore, it is imperative that the IS Auditor use good business sense and take into consideration the various business and IT alternatives within their organization in developing their level of activity and participation with the systems acquisition project team.

Request for Information (RFI)

This is the forerunner to the Request For Proposal (RFP), a document which identifies the business and operations requirements for an application system. The RFI phase is an opportunity for the organization to research and determine the type and application systems features available in the vendor application systems marketplace. It is suggested that the IS Auditor assure that required security, audit, control, and regulatory requirements for the system be part of this research and identification effort. Often users will learn from the vendor's response of interest about other system features that they may not have considered in their initial requirements. This is also another opportunity for users to determine if desired system functionality is in compliance with their organization's policies, standards, and IT infrastructure.

Request For Proposal (RFP)

This is the detailed document identifying the business unit, IT, and other stakeholder requirements, for an application system to meet the business need of the organization. The entire project team should be heavily involved in this phase of the project to assure that all business, operations, and IT requirements are fully defined, and represent the actual needs for the application system. The earlier these requirements are finalized before the selection process, the more time and money is saved by the organization by avoiding "additional requirements" – after the selection process has begun. This phase provides the IS Auditor with the opportunity to participate in the project by reviewing requirements with the project team, business sponsor, and key project stakeholders. This review process would include determining the completeness of requirement identification and the level of RFP review performed by the organization's legal department. This is a critical step, since if there are problems with vendor performance it will be necessary to have the legal department's interpretation of the vendor contract terms and conditions. The Project Risk Management Process should also be a part of this audit review, to assure that risks have been identified and that a risk mitigation process is in place and regularly monitored by the project management team and the business project sponsor.

If the audit review finds that the project team has not completely identified all stakeholder requirements, or an effective project risk management process is not in place, then the IS Auditor should prepare a document that raises these issues and discuss them with the project team and project sponsor.

Soliciting Responses to the RFP

An important process, since thorough research must be done by the project team to identify potential vendors and like organizations having a similar or the same business need, as the organization. Too frequently organizations will only send their RFP to well-known vendors and overlook other potential vendors that may have a better business and technology solution. This is often the case when RFI research and analysis is not thorough or is cut short due to project time constraints. Some vendor solutions that may meet most of the requirements may not be selected due to long time to delivery, or not being able to meet the organization's non-business or technical requirements (i.e. security, audit, regulatory). Often these are the vendors with a product that best meets the business requirements. Thus, it is important for future decision making in this process that the project team work closely with stakeholders to rank the priority of requirements from critical, essential, or optional. IS Audit should participate in this process to assure that all appropriate application system controls are not ignored by the project team.

Preparing for Rating Vendor Responses to the RFP

This phase is the basis for the contract to be completed with a vendor. The importance of ranking the requirement priorities is now apparent, since a single vendor will not be able to provide a 100% solution to the RFP requirements. The biases of the various project team members will most likely be exhibited in this phase, when determining which requirements are met and those which are not. It is imperative that a ranking methodology be developed in advance by the project team to score each vendor's ability to meet the RFP requirements. The requirements ranking methodology used must be agreed to by the entire project team, and the priority of each requirement must be a part of the scoring process. Another key document to consider at this point is the drafting of a Service Level Agreement (SLA) that identifies the organization's performance criteria and expectations of the vendor provided application system. This is also a good time for the entire project team to start drafting the User Acceptance Test (UAT) plan. It is

suggested that the IS Auditor, at a minimum, review and comment on the SLA and UAT since familiarity with these key documents will assist in identifying any control deficiencies in other project phases.

Project Management Reviews

During the period that vendor responses are being developed to the RFP, the IS Auditor has the opportunity to evaluate the overall performance of the project team to date. Using the project plan as a benchmark, the IS Auditor should compare project team performance against the project plan, including the project risk management tasks. The review should ensure compliance to required project policies, standards, and milestones. Project documentation should also be analyzed for completeness and adherence to organization standards. Another area for review by the IS auditor would be the project change control process. Some of the changes to review would include; project budget, requirements, addition of resources, changes in project team members, and changes in system performance requirements. Other documents that should be available for review are the Data Conversion Controls Plan, Project Risk Management Evaluation Reports, and any modifications to the original Project Plan.

All issues identified by the IS Auditor should be thoroughly reviewed with the project team for concurrence, and a final review report directed to the project sponsor and senior IT management. The IS Auditor should report periodically to management on progress in resolving issues identified in the project management review.

Selecting a Vendor

This is the most critical, time consuming, and political, phase of the entire project. Although steps have been taken since the beginning of the project to use objective tools and research to identify the best solution for a new application system, at times subjective opinions come into play within the project team. Dilemmas arise due to the variety of solutions offered by the vendors. For example, an application system may meet all of the business unit requirements, however, the operating platform for the system may not be within the organization's computing standards. The process for dealing with these issues by the project team must be developed prior to reaching this phase of the selection process. Again, the importance of priority ranking the requirements comes into play.

Once the selection process has reduced the number of vendors to three or four, vendor presentations to the project team for additional information, and also to evaluate the actual performance of the application system at an installed site, are scheduled. These vendor presentations are an excellent opportunity for the IS Auditor, since these interactive demonstrations provide additional system and vendor information and allow for unending questions on system operation, functionality, and performance – and control compliance.

Frequently the vendor scoring methodology will identify two final vendors – even if this is not the case, and only one vendor outscores the others, due diligence should still be performed on the selected vendor. The IS Auditor can be an important asset to this process since this type of analysis is frequently done by the audit department. Other members of the audit department can assist in this process, especially with performing financial and operational reviews.

Suggested areas for due diligence review would include the following:

- Review of audit, regulatory, and SAS 70 reports on the vendor
- Reference checking for customer satisfaction
- Review of existing vendor Service Level Agreements
- System audit documentation
- System security documentation
- Application internal controls documentation
- Vendor Quality Assurance Reviews
- D&B or other business rating reviews of the vendor

If the highest scoring vendor does not meet the due diligence review, then the project team must determine if the next highest scoring vendor should have a due diligence review. The IS Auditor should be closely involved with this process to assure that "exceptions" are not made to organization policy. However, in most organizations it is the prerogative of the business sponsor, to risk accept non-compliant issues with the vendor, or the vendor's application systems capabilities. This risk acceptance should be part of the project documentation and monitored by the project team, IS Audit, and the organization's IT Steering Committee (or equivalent executive committee having initiatives over-sight).

Vendor Contract Negotiations

This is often a time consuming process – not to mention expensive, since it involves the legal department of the vendor and the organization. The first issue becomes which contract form is to be used and then evolves until a final contract is signed. This is a good opportunity for the IS Auditor to provide important and independent background and research information to legal counsel. Due to the auditor's knowledge of both the business and technical requirements of the system, and attendance at the vendor presentations, they can also provide time saving access to project documentation. Issues the IS Auditor can specifically address in this phase would include the "right to audit clause," information security policy compliance by the vendor, meeting regulatory requirements, and system audit documentation. This last item is important since the IS Auditor will have to conduct an IS controls review of the application system in the future. If the system of internal application controls is not well documented by the vendor, then the IS Auditor will not be able to perform future application control testing.

The organization's vendor management policy should be well understood by the vendor to assure there are no conflicts over detailed requests for information or even on-site reviews by organization representatives. The IS Auditor should assure that, at a minimum, the vendors

compliance commitment to the organization's IS Security Policies, and full Regulatory Compliance (including commitments to meet future requirements) is met.

If a vendor acquisition project fails, for any reason, the vendor contract will be the basis for all non-performance issues. Therefore, it is important to ensure that specific conditions and terms are included within the contract or as a contract addendum. This is another area where the IS Auditor can add value to the project team by assisting legal counsel.

Data Conversion Plan

The data conversion plan is important for a new system because old system record formats and new system record formats are seldom compatible. This means that a detailed data mapping is needed to correctly re-populate the data to the new application system. In most cases, the vendor will have a tool to perform the mapping function, but it is not unusual for this mapping to be a manual operation. Probably the most critical part of the data conversion plan is the need to "scrub" the old data to assure that erroneous data is not transferred to the new system. This can be a very time consuming task since the additional work must be done by the business unit staff while concurrently performing their regular job function. If not well planned and organized, this task may take much longer and require more resources than originally planned by the project team. Also, if not done correctly, the organization may not know of problems until after the system is implemented and customers complain of inaccuracies. This creates a reputation risk for the organization. The IS Auditor can contribute with this process by reviewing the data conversion plan and determining if the controls and quality assurance over this process are satisfactory – to mitigate the transfer of corrupted data to the new system.

Systems Testing Phase

As with most new systems, the testing plan requires the attention and participation of the entire project team and the stakeholders. Some types of tests are not required for an acquired system, such as unit testing. Other types of tests are mandatory and would include interface testing, integration testing, and user acceptance testing. The IS Auditor, if not directly participating in the testing process, should review test results documentation and discuss any conditions or processes, that may not have been tested. If all testing is successful (defined in the test plan), then a final review by the legal department, for the vendor's compliance to contract terms and conditions should be performed.

System Implementation Phase

Upon the completion of all the previous phases identified above, the final step is to implement the system in the organization's production environment. Since deadlines and eagerness to complete the project are paramount to project team members, there may be some issues that are not addressed before the system cut over. The IS Auditor can independently identify some of the overlooked areas and advise the project team on incomplete or missed project tasks. Issues to consider include:

- completion of all documentation
- documentation on negative test results and the action plan to address errant conditions
- is the application now under the organization's user access authorization system
- have all stakeholders met, and do they all agree the application is ready for implementation
- have all vendor milestones been reviewed for completeness

In many organizations, new systems are run in parallel with the old system to assure that functionality and performance are satisfactory. This is an excellent practice, however, it does require users to perform "double duty" since they must now run the transactions through two systems versus one. This impacts everyone from data input staff to the accountants reconciling any differences between the systems. It is important that vendor representatives are on-site, or readily available, to work with the conversion team to assure that utilization of the system is correct and any system deficiencies are documented.

A final important task is for the entire project team and all stakeholders to meet and discuss "lessons learned" from the project life-cycle and the overall vendor performance. The IS Auditor should participate in this meeting since it provides insight into potential control deficiencies that will need to be addressed in audit's post-implementation review of the application system. An often overlooked area is for the project sponsor to prepare a document which identifies the measures in place to determine the achievement of the cost/benefits under which the project was approved by executive management.

Conclusion

An acquired system can be as complex a process as developing the application system in-house but with less control due to reliance on the external vendor. An organization that acquires a new system must carefully manage the project and not have it directed by vendor personnel. This article has identified some considerations for the IS Auditor to be involved with, to assure that the project is successful, and the organization is protected throughout the process, and the new application system is well controlled and effective in meeting the business need of the organization.

About the author
Doug Feil is a past president of the San Francisco Chapter of ISACA. He has more than twenty years of experience in IT audit consulting with major organizations in California and Hawaii. Doug co-authored a book, *Security and Control in an ORACLE® Environment*, by Dean Kinglsey, Sandra Carrier and Douglas Feil.

MEMBERSHIP

Hector Massa
Committee Chairperson

The membership count for the San Francisco Chapter as of May 1, 2002, stands at 359 members.

Please join me and the San Francisco ISACA Board of Directors in welcoming the following new chapter members.

Kemuel L. Bellows, CA,CISSP
Fairfield, CA

Carey A. Carpenter, CISA,CPA
Deloitte & Touche LLP
Transferred from Greater Hartford Chapter

Peter B. Eggenberger, CISA
Federal Reserve of SF
Reinstated Member

Kimberly A. Martens
Lawrence Berkeley Natl. Laboratory

David M. McCandless
Fortel, Inc.

Ferry Prajogo
Parkside Postal

Jason M. Purcell, CISSP
Exodus Communications

Chuck N. Reinhard
San Francisco, CA
Transferred from South Florida Chapter

Stephen L. Tin
San Francisco, CA

MEMBER MILESTONES

Members for over 25 Years

Douglas A. Webb, 1976
Charles A. Dormann, 1977

Members for over 20 Years

Gary W. Riske, 1978
David L. Lowe, 1978
Hector L. Massa, 1978
Charles C. Wood, 1979
Arnold Dito, 1979
David R. Durst, 1979
Robert C. Kimball, 1980
William Z. Davidson, 1980
Bob Gligorea, 1980
Carol Muller, 1980
Joel L. Lesser, 1981
William G. Martin, 1981
Kathleen W. Williams, 1981
Bruce L. Reid, 1981
Peter Hsieh, 1982
Judith Wall, 1982

Members for over 15 Years

Kathryn M. Dodds, 1983
Allen H. Martins, 1983
Kerry G. Elms, 1983
Leslie D. Fondys, 1983
Katherine M. Ullman, 1984
Jerry K. Hill, 1984
Martin W. Taylor, 1984
Richard J. Tuck, 1985
David A. Gilliam, 1985
Nancy D. Wiesbrook, 1985
Marcus A. Jung, 1985
Stephen Banks, 1986
Mary J. Bean, 1986
Steven Hudoba, 1986
Eugene W. Menning Jr., 1986
Vickie P. Smith, 1986
Paley Y. Pang, 1986
Kelvin Patterson, 1986
Louis R. Walker, 1987

Members for over 10 Years

Guy T. Anderson, 1988
Robert C. Motts, 1988
Sharon Tatehara, 1988
Jeffrey P. Mazik, 1988
Adam F. Levine, 1988
Ralph G. Nefdt, 1989
Kathleen E. Arnold, 1990
Beatrice K. Ashburn, 1990
Jack B. Cooper Jr., 1990
Todd E. Fenner, 1990
William Grant, 1990
Robert W. Hiday, 1990
Wing K. Yeung, 1990
Lawrence A. Jewik, 1990
Juan I. Lorenzo, 1990
Melody Jean Pereira, 1990
Keith D. Scott, 1990
James H. Tanner IV, 1990
Lawrence B. deBerry, 1991
Lynne A. Trestrail, 1991
Douglas K. Walsch, 1991
Leah J. McKern, 1992
J. Michael Samuel, 1992
Aidan M. Collins, 1992
Neville R. Morcom, 1992
Myoung Andy Kim, 1992
Foong Meng Wong, 1992
Scott W. Van Tyle, 1992
Lance M. Turcato, 1992
Richard M. Buford, 1992
Alec J. DeSimone, 1992
Jeffrey A. Nigh, 1992
Michael J. Cuggino, 1992
Carol A.Tanner, 1992

ACADEMIC RELATIONS

Brian Alfaro
Committee Chairperson

In continuing the tradition of providing aid to the student chapter of San Francisco ISACA, the Academic Relations Committee has been able to provide programs that were initially planned for in the beginning of this year: Scholarship Awards and the Internship Program.

As a reminder, it is important that the parent chapter maintains its strong relationship with the student chapter. The relationship among students can clearly be seen through the San Francisco State and San Jose State University students who were previous Board members and Directors and have contributed to the parent chapter, subsequent to their college careers.

First and foremost, congratulations should be announced to the distinguished students who have been awarded the CISA Review Scholarship for 2002. Although it was decided that only two students were to be awarded this scholarship, three students greatly displayed a high standard of scholastic performance, interest in the IT assurance field, and have overcome great adversity in their college career. Because of the students' performance, it was difficult to decide which two students should be awarded, and instead, all three students were awarded the scholarship.

The following students should be recognized for their great work and being awarded the SFISACA Scholarship: **Stephen Tin**, **Laura Ma**, and **Jun He**.

Special thanks should go to the Board of Directors for granting an additional scholarship, as well as **Todd Weinman** and **Kathleen Arnold** for helping to review student applications.

The Internship Program initiative set forth this year with the student chapter is always looking for companies and organizations to offer any positions to students to give them relevant experience in the IT assurance field. Special thanks should go to Kathleen Arnold at Sun Microsystems for helping to refer and assist in placing students in this program.

STUDENT CHAPTER

Carrie Chun Li
Student Chapter President

During the Spring 2002 semester, the Student Chapter was growing up very fast. I would like to recognize the organization's achievements and thank those whose hard work and perseverance made those achievements possible.

In this semester, we have 18 members, most of them are new members, which we recruited this semester. All the officers attributed to the intense recruiting effort planned. We did classroom presentations, direct mailings, and information tables to let more students know about ISACA and the benefits of being an ISACA member. We also successfully organized one workshop and two technical presentations in this semester. All these events help students to know about "IT Auditing Track" at SFSU and get real insight about IT audit. During this semester, we set up scholarships and provide internship opportunity for our members. Under our VP of Web Design – Stehpen Tin's hard work, our Web site and bulletin board are more rich and updated than before.

None of these achievements would have been possible without the combined efforts of ISACA student officers, members and local chapter. I would especially say "thank you to Mr. **Brian Alfaro**," who is the Academic Relations Chair in the ISACA-SF Chapter. He spent a lot of time with us to plan and became a main "bridge" between the Local Chapter and the Student Chapter. He set up internship and scholarships program for the Student Chapter, which attracted more students to be interested in being ISACA members. He also came to our campus to do the great "IT Auditing" presentation for us. Professor Edmund Lam and professor Jaime Eng (Chair of ISBA Department at SFSU) gave us very useful advice. ISACA Local Chapter President **Todd Weinman** and Mr. **Sumit Kalra** always supported our student chapter in the past few semesters. I want to thank you all for your support and help.

It has been a pleasure and honor to have had the opportunity to serve as the President for the student chapter for Spring 2002. I believe that our students' chapter will have a bright future under the efforts of the new student officers, members and local chapter.

Apologies for e-mail glitch

On a couple of occasions over the past month, some of you may have received e-mail notices for education events that have already occurred. We here at ISACA have not lost our minds, though at times it seems that our e-mail server may have. This glitch occurred during repairs to the server used to send e-mail announcement of Chapter events, and it resulted in the re-sending of countless old e-mails that had already been sent. We are hopeful that we have the problem resolved and apologize for any confusion or inconvenience it may have caused.

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 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 hlmsa@aol.com to ensure that you receive important information electronically.

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

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

CORPORATE SUPERSTARS

by Todd Weinman

Todd Weinman is the current President of the San Francisco Chapter of ISACA. He is an executive recruiter and Western Regional Director for Lander International, the world's largest recruiting firm specializing in IT Audit.

Todd enjoys visiting audit, information security and consulting departments all over Northern California, and he is in contact on a daily basis with scores of directors, managers and staff level professionals from around the region.

A frequent speaker for ISACA, the IIA and local universities, Todd is a graduate of UC Berkeley and worked for a large CPA firm prior to joining Lander International. Todd was selected as the 1999 CAPC Consultant of the Year for the state of California.

Company sponsorship and support is critical to the success of a volunteer professional organization. Corporate sponsorship, for example, allows the chapter to present educational and/or other offerings at a price that is more reasonable to the member by offsetting key fixed costs. Companies can also provide assistance by encouraging their employees to present at educational events or by assisting in the many tasks that are involved in the successful functioning of a thriving Chapter. In this section I would like to acknowledge those organizations that were strong contributors to the Chapter over the past years.

Gold Medal

First, I would like to offer my great appreciation to **Bank of America** for their support in a multitude of areas. Coming in as Chapter President, one of my goals was to get more involvement from one of Northern California's most important IT Audit departments; in return they delivered above and beyond expectations. Thanks to the outstanding efforts of **Rick Beckman** and **Dave Lufkin** among others, Bank of America supplied speakers for several of our educational events, including the Fall Seminar (some of whom flew in from Dallas just to speak at the event), the joint ISACA/IIA seminar and the Full Day seminar held at the Bank of America facilities in Concord. Their presentations were among the best and most detailed that we received all year. In addition, contributions by BofA employees almost single-handedly enabled us to achieve our goal of significantly increasing the technical content of our newsletters. BofA also hosted countless conference calls saving money for the Chapter.

Our other outstanding contributor this past year was **PricewaterhouseCoopers**. Back in the embryonic stages of planning our Fall Seminar, we were not certain whether we could pull the event off and we were concerned about the financial risk to the organization. **Rick Biehl** and PwC stepped up without hesitation to provide a $2500 sponsorship of our Friday luncheon. Just to offer some perspective, this essentially amounted to a $50 discount to each of the nearly 50 people who attended the Fall Seminar. PwC also provided a number of speakers for our educational events.

Silver Medal

Another strong contributor to our Fall Seminar was **Captus Networks**, which sponsored our Thursday luncheon. Captus also provided speakers for several of our education events.

Bronze Medal

Deloitte & Touche deserves recognition for providing speakers for a number of our education events. They also assisted by hosting numerous conference calls, and they assisted with printing needs.

Mike Villegas and **iSecure Privacy** sponsored a meeting break at our Fall Seminar, and Mike was one of our presenters.

If there were an award for supporting the Chapter by sending employees to our education events, it would surely go to **Kelvin Patterson** and **Providian Financial**. Kelvin sent nearly his entire staff to both our Fall Seminar and North American CACS. Good work Kelvin, keep them coming!

Finally, I would be severely remiss if I didn't mention my own organization, **Lander International**. Anyone who has ever employed a President of a professional organization knows the unbelievable time demands that are involved. **Richard Tuck** could not have been more supportive and understanding of how these demands sometimes deterred my focus from my duties at Lander. In addition, Lander provided sponsorships of both the Fall Seminar and an SFSU student chapter event. But perhaps most important is the amazing support I received from my Lander team members, particularly **Helen Winters** and **Frank Biafore**. They have put in countless hours, creating and sending our education event announcements, coordinating event registrations, and a variety of other tasks, much of it under tight time deadlines. They never once complained and they always came through. I could not have performed my duties this year without their tremendous support.

SF ISACA LUNCHEON, PROGRAM, AND ANNUAL MEMBERSHIP MEETING

Organizational Design for Information Security • Thursday, July 18, 2002 • 1.5 hours of CPE credit

Session description

Still an embryonic field, information security is considered by many people to be strictly a technical computer specialty. While technical issues are certainly important, what gets left out by many managers are the people factors such as organizational design. As a result, these managers don't know who should be doing what tasks, and information security matters are either neglected or grudgingly attended to. Coming back to the centrality of properly managing for information security, Charles Wood will discuss ideas from his new book entitled *Information Security Roles & Responsibilities Made Easy*. These topics will include the benefits of clarifying roles and responsibilities, the need for a team approach to information security, alternative reporting relationships for information security, staff motivational techniques, and information security-related outsourcing contracts.

Speaker bio

Charles Cresson Wood, CISA, CISSP, is an independent information security consultant based in Sausalito. He has worked in the information security field since 1979 including stints as a computer crime researcher (at SRI International) and as an information security officer (at Bank of America). Since 1985 he has provided custom management consulting services to a commercial firms including banks, telephone companies, utilities, and airlines. His work with over 125 clients has taken him to over 20 countries around the world. He has published over 225 articles and six books dealing with information security (he is best known for his book and CD-ROM entitled *Information Security Policies Made Easy*).

Register

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

Schedule

Time	Description
11:30-noon	Registration
11:30-12:30 pm	Lunch
12:30-2:00 pm	Presentation
2:00 - 3:30 pm	Annual Membership Meeting

Pricing (including Saver Pass info if applicable)

$40 Members (or 1 Saver Pass)
$50 Non-members (or 1 Saver Pass plus $10)
$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

by Dan Hilton, Vice President, Technology Audit Consultant, Bank of America

The Unix operating system is widely used today to host applications throughout many different organizations. If your organization fits in this category, then internal audit should take an active role in auditing these systems. The Unix operating system has many capabilities and functions that if not adequately secured or "hardened" can be plagued with many vulnerabilities and open doors. Many auditors realize this is a potential risk and conduct a variety of general control reviews. These audits generally include a review of the process controls associated with each system, including; change management, problem management, and security administration. However, to ensure that the Unix system is truly hardened, a detailed configuration review should be conducted. This will be a three-part article that will highlight many of the items that should be reviewed during a Unix configuration audit. In subsequent issues, we will address user IDs, Unix services, exportable files, and several other areas of control.

Rhost Files

Description: The use of .rhost files is one method that can be used to login remotely to a Unix system. Within each .rhost file, there are two settings which indicate where the remote user must originate from, and who that user must be authenticated as on the originating system. If either of these settings are identified with a plus sign, then it is interpreted as any location and/or any person.

Control: These files should not exist on the system unless they are absolutely needed for normal business operations. The file should contain information that is specific to a particular system and person, plus symbols should not be used. In addition, the files should be restricted to be readable only by the owner.

These files can be used by unauthorized users to gain access to Unix systems. The level of access granted is dependent upon the owner of the .rhost file because the permissions of the .rhost file owner are inherited by the .rhost user.

File(s) to Review: All .rhosts files should be reviewed. The following commands need to be executed to review the controls discussed above.

```
find / -name .rhosts -local -print >>
rhost_files
```

The user should read the contents of the file created in the above action. This can be done by the following command:

```
cat rhost_files
```

To determine the permissions set on these files, the user must run a command against each file name listed in the rhost_files file. This can be done by using the following command:

```
ls -al [enter individual filename here]
```

A few examples of this would be the following:

```
ls -al /.rhosts
ls -al /home/jdoe/.rhosts
```

Netrc Files

Description: Netrc files are used to automate an ftp process. For an ftp process to occur, a user ID and password must be available. Therefore, the contents of a .netrc file contain a user ID and password, which is stored in clear text.

Control: The use of .netrc files is not recommended, unless they are imperative for normal business operations. If needed, the file should have permissions that only allow the owner to read the contents of the file.

These files are often used to obtain user IDs and passwords from the contents of the file, which can then be used to gain unauthorized access to system. The level of access granted is dependent upon the owner user ID and password that is displayed in the .netrc file.

File(s) to Review: All .netrc files should be reviewed. The following commands need to be executed to review the controls discussed above.

```
find / -name .netrc -local -print >>
netrc_files
```

The user should read the contents of the file created in the above action. This can be done by the following command:

```
cat netrc_files
```

To determine the permissions set on these files, the user must run a command against each file name listed in the netrc_files file. This can be done by using the following command:

```
ls -al [enter individual filename here]
```

A few examples of this would be the following:

```
ls -al /.netrc
ls -al /oracle/db/.netrc
```

Hosts.Equiv Files

Description: Like the .rhost file, the hosts.equiv file is also a trusted host file. The file is set up so that users authenticated to other systems can connect to the system containing the file, without a password. The file will contain the names of other hosts that are "trusted" by the system with the hosts.equiv file. A user would connect to the trusting system by using rlogin or rsh.

Control: The use of hosts.equiv files is not recommended unless they are needed for standard business operations. If needed, the file should have permissions that only allow the owner to read the contents of the file. In this case, the owner should be the root account.

A hosts.equiv file can be used to gain unauthorized access to a Unix system. The access level that is granted is based upon the user rights of the id that is being matched against the remote system.

File(s) to Review: To review the contents of the hosts.equiv file, executive the following command.

```
cat /etc/hosts.equiv >>
host.equiv_files
```

To determine the permissions set on the hosts.equiv file, use the following command:

```
ls -al /etc/hosts.equiv
```

Login Banner

Description: When a user is attempting to login to a system, a banner typically appears that warns users trying to gain unauthorized access.

Control: The organization should have a standard login banner that has been approved by the company's legal department. See the following example:

"To protect the system from unauthorized use and access, activities on this system are monitored, recorded and subject to review. Any unauthorized access to this system is prohibited and all offenders will be prosecuted."

Evidence of a warning banner is needed when trying to prosecute an individual for gaining unauthorized access. Some cases have resulted in dismissal because it was not present on the system.

File(s) to Review:
Solaris: cat /etc/issue
The banner should be stated in this file.

AIX: cat /etc/security/login.cfg
The herald section should contain the banner.

HP: cat /etc/motd
The banner should be stated in this file.

Password Settings

Description: Passwords are one of the keys to ensuring only authorized users are accessing systems. Often, password controls are extremely lax so users can easily remember their passwords and do not have to change them. Unfortunately, this often results in a majority of users establishing weak passwords (i.e. user ID = password). Solaris, AIX, and HP all have specific configuration parameters, which allow administrators to add restrictions to passwords to prevent this problem.

Control: The organization being audited should have standards that outline password policies and requirements. These should be used to audit against the settings on the Unix system. Typically, password benchmarks would include the following:

- Password length of no less than 7 or 8 characters
- Password should be changed every ninety days
- Passwords should include alphabetic and numeric characters
- A password history of 8 should be kept, preventing the reuse of passwords.
- A minimum password age should be set to one day to prevent the ability to circumvent password history controls.
- A user ID and password should be locked after five failed login attempts.

Different variants of Unix allow for more or fewer controls associated with passwords. See the section below for further details.

Inadequate password controls and weak passwords make it easier for unauthorized users to guess or crack passwords. Free tools are readily available on the internet to automate this task.

File(s) to Review:
Solaris: cat /etc/default/passwd

- **Maxweeks** Establishes the amount of time before a password expires.
- **Minweeks** Establishes the amount of time that must pass, following a password change, before the password can be changed again.
- **Passlength** Establishes the required password length.

AIX: cat /etc/security/user

- **Maxage** Establishes the amount of time before a password expires.
- **Minage** Establishes the amount of time that must pass, following a password change, before the password can be changed again.
- **Minalpha** Established the minimum number of alphanumeric characters that must be present in a password.
- **Minlen** Establishes the required password length.
- **Histsize** Establishes the password history
- **Loginretries** Sets the number of failed login attempts that must occur before a user id and password is locked.

HP: cat /tcb/files/auth/system/default

- **u_exp** Setting requires a user to change their password after a specified period of time
- **u_life** Setting will suspend a user ID if the password has not been changed in the timeframe specified in this setting
- **t_maxtries** Sets the number of failed login attempts that must occur before a user id and password is locked.
- **u_maxlen** Establishes the required password length.

Umask Setting

Description: The umask setting determines the permissions that will be set on files when they are first created on a system. Often times, users do not take the time to ensure that the files they create on the system are restricted to the appropriate users.

Control: A minimum benchmark setting for umask should be 022. This indicates that when a file is created, the owner of the file has read, write, and execute privileges. However, individuals assigned to the group and the world only have read and execute privileges. (For a further understanding of the meanings of group and world, see the recommended references below). A more restrictive benchmark setting would be 077. This would allow all privileges to the owner, but no privileges to the group and world classes. The setting should never be set at 000.

The failure to set the umask setting can result in permissions that allow inappropriate access to files.

File(s) to Review:
Solaris: cat /etc/default/login
See umask setting in this file

AIX: cat /etc/security/user
See umask setting under default

HP: Each individual user can have a different umask setting. To prevent individual settings, administrators can set umask in each user's .profile file. Ask a system administrator to review a sample of .profile files for the following setting: "umask 022"

HARDENING THE UNIX SYSTEM – continued

These are certainly not all the potential vulnerabilities on a 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/

This article focused on only some of the key areas that should be reviewed during a Unix configuration audit. In the next two issues, we will address user IDs, Unix services, exportable files, and several other areas of control. Reviewing the settings in this and subsequent articles, along with using the recommended resources should improve your understanding of how to help secure a company's Unix systems. Your company will benefit from a comprehensive review to reduce the security and reputation risks associated with Unix systems.

2002 CISA INSTRUCTORS by Sumit Kalra, CISSP, CISA

The San Francisco ISACA chapter would like to thank the CISA instructors for sharing their time, knowledge and expertise.

- Carey Carpenter
- Todd Weinman
- Sumit Kalra
- Edmund Lam
- Joshua Mock
- Douglas Feil
- Stuart White
- Maria Shaw

2002 CISA Examination

The International Chapter of ISACA administers registration for the CISA examination. The 2002 CISA examination was scheduled for Saturday, June 8, 2002. Visit ISACA International at www.isaca.org to obtain more details. GOOD LUCK TO ALL OF YOU!!!!!!!!!!!!

2002 CISA Review

The San Francisco Chapter offered a complete review course for the 2002 CISA examination. This review course was designed to assist candidates in preparing for the CISA examination. The review sessions were taught by IS audit, control and security professionals and include lectures, classroom discussion, practice exams, coffee, Krispy Kreme donuts, Noah's bagels and orange juice. The four-hour review course sessions were held over eight Saturday mornings in downtown San Francisco.

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. Brian Alfaro led the CISA Coordination committee.

To be continued...look for part II of this article in the next quarter newsletter.

Accolades for the CISA Class

From Doris Fung: "I want to thank you for coordinating the CISA class. It was well-organized and lots of fun too. The best thing is that it helps to keep our spirit high. I think you guys have done a great job whether or not I could pass in the exam."

NORTH AMERICA CACS WAS A SUCCESS

by Beverly G. Davis, CACS Conference Chairperson

The Chapter and all its colleagues from around the globe came together at the Fairmont Hotel and indulged in this outstanding knowledge exchange. Participation feedback from the attendees, presenters, exhibitors, and volunteers was all so positive. Most of all, the San Francisco weather throughout the week was just perfect.

The conference content covered the following areas: Enterprise Resource Planning Applications, Wireless Technologies, IT Risk Assessment, E-business, Information Security, and COBIT.

We had four days to enhance our skills in many of the core competencies for IT Audit professionals. This event was made possible by the members of ISACA and international.

On behalf of the Chapter we would like to express our sincere appreciation to the members and volunteers for the contribution to the conference success. Special thanks are extended to the following volunteers:

Gloria Lievano
Marc Jung
Christina Cheng
Todd Weinman
Swee Fuller
Kathleen Arnold

The individuals listed above were members of the coordinating committee. Thank you!

A very special thanks to the following individuals who gave of their time to volunteer during the conference:

Carrie Li
Benjamin Chao
Stephen Tin
Wendy Leung
Colin Lau
Lucy Syamsu
Doris Beers
Chuck Dorman
Helen Sun
Hector Massa
Anne Woodbury
Jerry Bennett
Erin Andrews
Alan Wong
Romelle Parsons
Terri Lowe
Kendell Tieck
Terru Bexdek
Kim Brown
Sandy Rhein
Dwayne Henderson
Bill Davidson
Eleanor Lee
Allen Martin
Anna Chan

To all of you thanks because without your efforts the conference would not have been a success!

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

2nd Vice President
Rick Beckman
Bank of America
925-675-5282
rick.beckman@bankofamerica.com

Treasurer
Anne Woodbury
925-944-5982
annewoodbu@aol.com

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

Directors

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

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

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

Edmund Lam

Hector Massa
Office of Thrift Supervision
650-746-7138
hector.massa@ots.treas.gov

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

Committees

CACS 2002
Beverly Davis, Chair
Kathleen Arnold
Swee Fuller
Steven Hudoba
Marcus Jung
James Kastle
Edmund Lam
Gloriea Lievano
Eva Paiva
Todd Weinman

CISA Review
Sumit Kalra, Chair
Brian Alfaro
Helen Sun

Communications
Christina Cheng, Chair
Brian Alfaro
Doug Feil
David Lufkin
Maria Shaw
Aron Thomas
Lance Turcato
Todd Weinman

Education
Rick Beckman, Chair
Carey Carpenter
Anne Cole
Deb Frazer
Steven Hudoba
Jim Kastle
William Luk
Todd Weinman
Stuart White

Membership
Hector Massa, Chair

Advisory Board

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

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