Information Systems Audit and Control Association

SAN FRANCISCO CHAPTER LOCAL AREA NETWORK

FIRST QUARTER 2005

Winner of the 2000 Wayne K. Snipes Award – Best ISACA Chapter in the USA and the World
Winner of the 1999 Newsletter Contest – Best Newsletter for Large Chapters in North America & Worldwide
Winner of the 2000 Newsletter Contest – Best Newsletter for Large Chapters in North America
Winner of the Outstanding Web Site Award – 2003 Gold Level; 2001 and 2002 Silver Level

PRESIDENT'S MESSAGE

Lisa Corpuz
President

Contents

Welcome 2005 and Happy Anniversary SF Chapter!

It's hard to believe that we are well into the new year! Months feel more like weeks and days are more like hours. I know that 2004 has been a busy year with all of our work commitments and this year will be no different. We appreciate your continue participation in all the past year events and activities and look forward to seeing you more in 2005.

As you begin to read this newsletter, you will find that we have many activities schedule this year. I have highlighted some of the key events below and I hope that you will take the opportunity to participate in these events and better yet, to volunteer your time by helping out the various committees:

San Francisco Chapter 30th Anniversary

Without saying, this year is a special year. It is the 30th year anniversary of the Chapter. Happy Anniversary! Not only will we continue our commitment to provide excellent monthly sessions, the Fall conference, certification review courses, and our newsletters, just to name a few, but we are also planning a special event to celebrate our 30th anniversary. So stay tune for upcoming announcements and if you have any suggestions and ideas as to how we can make this a memorable anniversary year, feel free to contact any of the board members, officers or committee chairs.

Best Paper Contest for Professionals and Students

We are offering another exciting year for the best paper contest. If you have a talent for writing and have an IT security or audit topic that you would like to write about, this is the perfect opportunity for you. Entry submission deadline for both professional and student papers is May 16, 2005.

CISA and CISM review courses

The SF chapter is offering another year of CISA review courses. This year the CISA course will be held at the Wells Fargo training conference rooms beginning Saturday April 9th through June 4th. As our records have shown, we have been successful in our CISA courses with a high percentage of chapter member passers. Many of the instructors are members of the chapter and have donated their time to present sections of the review course to the class. For the first time this year we will be offering a CISM review course as well. If you are considering pursuing a certification, don't overlook these review courses. The price is right and the benefits are overwhelming.

Monthly Education Events

The SF Chapter continues to offer monthly education events for our chapter members. In addition to our luncheon events, we will offer two full day sessions this year. In January, we recently held our first full day session on Windows, Active Directory and Forensics and were fortunate to have Rodney Kocot and Richard Chew as our guest speakers. Our next full day seminar is on Business Continuity Planning and is scheduled for March 31st. This is a joint event with Business Recovery Management Association (BRMA) and will be held at the SBC building in San Ramon. Stay tuned for more details on our upcoming events.

Web site Revamp Project

With the guidance of our webmaster, we are currently in the process of revamping

PRESIDENT'S MESSAGE – continued

our Web site. Our goal is to make our Web site more user friendly with the resources and tools needed to navigate through the Web site. Also, we are working on improving the Web site so that our information about chapter activities current and useful to our members. If you have a talent or interest in assisting in this Web site project, please contact the webmaster or any of the board members.

As you can see, we have a busy year ahead of us, and this is just a short list of what is ahead. I hope that you will take advantage of all that is offered this year and participate in our events. Feel free to contact any of the Board members or committee chairs listed in the back of this newsletter with your suggestions and comments. We are here to serve our members and your feedback is very valuable to us!

CISM REVIEW COURSE

Questions we should be asking ourselves everyday:

1. How can I provide senior executives the assurance that I understand the interwoven relationship between business needs and IT security?
2. Which certification focuses on info-security governance, enterprise program management and global security strategies?
3. With the many certifications out there, which is the one that truly reflects my security management credential?

The answer is:

CISM

(Certified Information Security Manager)

CISM, the Certified Information Security Manager, is ISACA's next generation credential and is specifically geared toward experienced information security managers and those who have information security management responsibilities.

The CISM designation is designed to provide executive management with assurance that those earning this certification have the required knowledge and ability to provide effective security management and consulting. It is for the individual who must maintain a view of the "big picture" by managing, designing, overseeing and assessing an enterprise's information security. It is business-oriented and focuses on information risk management while addressing management, design and technical security issues at a conceptual level. While its central focus is security management, all those in the IS profession with security experience will certainly find value in CISM.

The CISM examination is recognized in numerous publications, for example, SC Magazine and Information Security Magazine, as a unique new management credential. In November 2003, Certification Magazine recognized CISM among its "top ten" Best New Programs or Certifications. Prominent CISM's include Howard A. Schmidt (eBay), Eugene Schultz (Lawrence Berkeley National Laboratory), Robert Clyde (Symantec Corp.), just to name a few.

The CISM examination consists of 200 multiple choice questions to be administered over a four-hour period. Questions are designed to test practical knowledge and experience. The areas covered under the examination are:

- Information Security Governance (21%)
- Risk Management (21%)
- Information Security Program Management (21%)
- Information Security Management (24%)
- Response Management (13%)

The next CISM examination will be offered on June 11, 2005. Registration deadlines are as follows:

- Early Deadline: February 2, 2005
- Final Deadline: March 30, 2005

Register online and save US $30!

Bulletin of Information and details of the examination are available at the ISACA Web site at www.isaca.org.

The San Francisco Chapter is proud to announce that a 2-day CISM Review Course will be coming to the Bay Area in 2005. Although it will be our first year, we are committed to getting the best instructors and providing examination-taking tips for CISM-to-be in preparation for the examination.

If you are interested in knowing about our CISM Review Course, please contact me at chricheng@deloitte.com or (408) 704-4203.

Respectfully submitted by
Christina Cheng, Past President
CISM Review Course Coordinator

Information Systems Audit and Control Association®

A recognized global leader in IT governance, control and assurance.

SAN FRANCISCO CHAPTER CISA REVIEW COURSE

BECOME A CISA – ENROLL NOW!

Early registration deadline: February 18, 2005

Registration deadline: April 9, 2005

9 AM - 1 PM on Saturdays • April 9 - June 4, 2005

Classes held at Wells Fargo Services

155 5th Street, First Floor • San Francisco, CA 94607

Member Early Bird	**$250**
Member	$280
Non-member Early Bird (including 1 year ISACA membership)	**$400**
Non-member (including 1 year ISACA membership)	$440
Full-Time Student Early Bird	**$150**
Full-Time Student	$180
Part-Time Student Early Bird	**$180**
Part-Time Student	$200
Partial enrollment for non-members (per class)	$60
Partial enrollment for Members (per class)	$40

Got questions? Contact Conny Cheng at cocheng@deloitte.com or (415) 783-4176

For more information, visit www.sfisaca.org/cisa/review.htm

Mark your calendars for our next full day seminar on Business Continuity Planning.

It is scheduled for March 31st. This is a joint event with Business Recovery Management Association (BRMA) and will be held at the SBC building in San Ramon.

Check www.sfisaca.org for details.

246386

SECURITY FLAWS IN YOUR ENTERPRISE BUSINESS APPLICATIONS

The hidden threat to "Business as Usual"

As business has shifted from face-to-face interactions to anonymous electronic transactions the impact of hackers and malicious insiders has risen to epic proportions. Most businesses are now "boundary-less" through the proliferation of the Internet, networked computing, and ever-increasing levels of automation all enabled by software. The gains have been impressive, but the revolution's sword cuts both ways.

This reality has attracted, motivated and enabled hackers, criminals, and malicious insiders who attack and misuse business applications for malice and profit. And the trend of successful attacks is accelerating. Nearly every business-critical application deployed today contains vulnerabilities that can be exploited to cause considerable loss or business interruption. According to Gartner, "over 70% of security vulnerabilities exist at the application layer, not the network layer." It's not just operating systems or web browsers, but all types of applications. And since business applications often extend beyond a company's perimeter, traditional security measures aimed at protecting the network cannot adequately protect the software or the company.

Something must be done. Security must be introduced earlier into the software development lifecycle. This change will not come from simply proving that we have vulnerable code – we know that already. The solution is to fix the root cause of the security vulnerabilities in the applications themselves.

Software itself must become strong and protect itself from attack- its time to fortify our software.

Software security flaws – the menace lurking within

And business applications are likely more susceptible.

Mention software security vulnerabilities and the mind runs immediately to operating systems and the multitude of problems and billions of dollars of losses that hackers and virus writers have caused over the last several years. In the first three quarters of 2003, CERT reported 2982 operating system vulnerabilities (158 for Microsoft alone) – averaging more than ten a day.

With each revelation of a new security breach comes a fanfare of concerned computer users questioning why these attacks are so prevalent; how could software developers be so careless as to leave critical applications vulnerable and unprotected. It doesn't end at the operating system however. Security flaws are resident in the software that runs your business, and that software is even more likely to be susceptible.

The fact of the matter is that high-profile development efforts at Microsoft and other infrastructure technology firms demand and receive close scrutiny for potential vulnerabilities. And while highly publicized breaches in infrastructure systems can and often do impact businesses, these software vulnerabilities (the flaws that can be leveraged by the ever-growing ranks of hackers and malicious insiders) pale in comparison to those affecting the critical business automation software that most companies depend upon to operate. In a single year, the financial services industry writes more custom software than all the operating system companies have ever produced. And for each highly publicized vulnerability uncovered in Microsoft Windows, a hundred or more vulnerabilities lie undetected, embedded within the source code of even the most critical business applications.

Businesses are increasingly dependent on information technology, most to the extent that many simply could not operate without the software systems that automate their key business processes. The stock market, for example, requires linked business systems to execute trades between brokers and exchanges. Likewise, supply chains in most manufacturing segments would break down without the flow of information between suppliers and producers.

Telecommunications would certainly not operate without the ability to connect cell phones to the computers controlling the network and the billing systems.

Information systems are becoming progressively more complex, higher-powered, interconnected, and openly accessible to partners and customers over vastly distributed networks. Instead of personally conducting transactions face-to-face with known partners, much of our business now occurs across anonymous electronic channels. Add to that the fact that software development itself is becoming more distributed through offshore development arrangements and intra-company collaborative computing.

These trends strain the ability of organizations to secure and protect the very essence of their business – the systems, the information they contain, and the physical assets those systems manage – from misuse or unauthorized access. Attackers compromise "secure" systems every day.

Nearly every major business application deployed today contains vulnerabilities that can be exploited to cause considerable harm by external hackers or malicious insiders. These vulnerabilities can be leveraged to steal crucial information, sabotage computer systems, or influence processing for the profit or malicious intent of the attacker. Consider the impact of a worm like Mydoom or SQLSlammer that was able to infect systems around the globe in a matter of minutes bringing down key business systems at a total estimated cost of over $1B. Now imagine a targeted version of that attack against your most critical business systems leveraging similar software vulnerabilities – What operations could an attacker interrupt in your business? What data could they compromise? Many companies are oblivious to this risk and operate on the false assumption that their business software does not contain such vulnerabilities. Unless there is an active program to identify and mitigate security flaws, it would be foolhardy to assume business application code is free of the same mistakes routinely made by the pros.

Even though it is just being recognized,

the business impact and risk exposure of application vulnerabilities is enormous, and experts agree it's growing at an alarming rate. According to Gartner Research, "Over 70% of security vulnerabilities exist at the application layer, not the network layer. The most damaging targeted attacks have focused on vulnerabilities in Web applications and custom-developed software."

In 2002, the White House assembled a group of information security experts who delivered the National Policy to Secure Cyberspace. In that document they explain, "For the United States, the Information Technology Revolution quietly changed the way business and government operate. Without a great deal of thought about security, the nation shifted control of essential processes in manufacturing, utilities, banking, and communications to networked computers." They go on to state that, "cyber attacks on US information systems occur regularly and can have serious consequences such as disrupting critical operations, loss of business revenues and intellectual property, even the loss of life."

In spite of this incredible impact, it is the operating system vulnerabilities that are widely publicized, not business application software. The reason: most exploits continue to go undetected and unreported. Those that are exploited by hackers or malicious employees represent "bad press" for the companies involved and are, therefore, kept out of the public spotlight. In many cases, incidents are not even disclosed to senior management.

If the loss of vital data, interruption of critical business processes, and damage to a company's brand and reputation isn't enough, software vulnerabilities in critical information systems can even put you and your business on the wrong side of the law. Companies are now facing a growing range of complex regulatory statutes and liability laws around information security. Over the last several years, regulatory and law-making bodies ranging from the FTC and the SEC to state and federal lawmakers have put tough data privacy regulation in place in an attempt to protect consumers and enhance national security by shoring up systems that are critical to national infrastructure.

Response to date – focus on symptoms not the root cause

Tremendous resources are being deployed each day to reduce the risks posed by IT systems, but that effort continues to target the network perimeter. Information technology departments around the world are spending billions of dollars each year on state-of-the-art firewalls, intrusion detection systems, and 24x7 network security monitoring to prevent unauthorized access to business applications and their data. However, at the same time, these same enterprises are buying , building, and integrating proprietary and open-source code at a record pace and pushing it into production without a dedicated course of action to make sure the software itself is secure.

Leaders in defense, banking, telecommunications, healthcare industries, along with a few of the largest software vendors have responded aggressively to the threat posed by software security vulnerabilities. At the same time, the response has been slow in most organizations where solutions are poorly aligned with the root cause. Alarmingly, the response remains nonexistent in many key industries, including the broader computer software industry. There the cost of poor security is not absorbed by the software maker, but rather passed on to the customers – who are often unaware of the risk exposure they are accepting.

The most common misconception that befalls many companies is the false sense of security that comes from running mission-critical business applications "behind the firewall." Applying mainstream network security solutions, such as firewalls, to application security problems hinges on the premise that, by isolating it from the dangers of the outside world we can somehow protect exposed and vulnerable software.

Sealing off business applications from the "outside world" is simply no longer practical or even possible within the current business environment. Applications today are regularly and legitimately accessed by thousands, tens of thousands, or even in some cases millions of users. Businesses demand open access to programs by employees, suppliers, customers, and partners located around the world. Consequently, it's these new "boundary-free" business applications that make the firewalls porous. It is through these applications that hackers can most often reach and exploit vulnerabilities. The true flaw in the outside-in premise, then, is that vulnerable software can be protected at all – without addressing its inherent vulnerability at the root cause.

As organizations begin to recognize and confront software security issues, Quality Assurance (QA) and post-deployment Attack and Penetration (A&P) tests are often used to solve the problem. However, addressing software security exclusively as a testing problem fails in two ways. First and most fundamental is the nature of testing – A test logically follows some course of action and is used to make sure that course of action was successful. As such, a test can only confirm a desired result; it does not by itself produce that result. If a development team builds a complex piece of software and does absolutely nothing during the effort to mitigate software security vulnerabilities, what should we expect a test to yield?

Imagine, for example, giving a high-school Calculus test to fifth graders prior to any study of the subject – of course they will fail just as every single piece of enterprise software does today when tested for security vulnerabilities. Unbelievable as this may seem, this is the state of the art for many organizations that have begun to consider the security of their business applications.

Large companies routinely pay millions of dollars per year to perform post-deployment security tests against enterprise applications. Typically these are in the form of third-party "red team" attacks on key business applications. These red teams (or "ethical hackers") are, as you might guess, finding alarming numbers of vulnerabilities in virtually all business applications they test. This initial response to this software problem has been focused

on proving what we already know – we have security problems in our application code. The more important and elusive issue thus far is how to eliminate those security problems.

There is a secondary problem with considering software security problems as a Quality Assurance issue rather than a core development problem. Software Quality tests are traditionally focused on verifying a set of features as defined by some reasonably well defined requirements. Security testing requires a different mindset and approach for it is the absence of something, namely security vulnerabilities that we are looking for. This places a great burden on the tester, because they must know the universe of security vulnerabilities regardless of what our code is supposed to do – our testers must not only know the business domain, but they are now required to be as good as the best hacker. If a particular test indicates the software is secure, how can we know that the right tests were run?

Further complicating matters, in traditional QA, developers rely heavily upon end-users as a final line of defense for finding errors in newly developed software. This model is very cost effective and efficient – for the developer. Consider the most recently deployed software you use. Was it error free? Probably not – and if you reported errors back to the development team, then you played a crucial role in the overall QA effort.

Now consider a subtle security flaw discovered by a hacker. The last thing they would do is notify the developer of that issue – they will instead exploit the vulnerability for as long as they can. Unlike a functional quality issue, the developer will not receive notification from the user that finds these problems. Any safety net created by this process of user-reported software flaws is nonexistent when it comes to security vulnerabilities. Developers simply must not allow applications to ship with security vulnerabilities.

Whether it is post-deployment security testing, attack and penetration testing, or the analysis of binaries, waiting until applications have been built before addressing security vulnerabilities is fundamentally impractical. Finding vulnerabilities after the fact is far more difficult and costly. Software developers are the ones creating the vulnerabilities and they are the only ones with access to the source code and the ability to make the fix.

Testers are at a huge disadvantage to external and internal hackers who also have the benefit of time. Many, seemingly innocuous, vulnerabilities may not be exploited or exploitable by hackers at first deployment, but as software often remains in service for years, they pose a threat far into the future as other parts of the system change. The problem starts when the vulnerabilities are coded into the system – that is undeniably the most efficient and opportune time to remove them. The security of business applications must be the charge of the developers who build those applications.

We have software security problems – how do we drive solutions?

Given this situation, a question naturally presents itself: why are outside-in (network-based computer security and post-deployment testing) solutions applied to what is clearly a software development problem? The answer – today's development teams are not leading the charge. Rather, it is the security professionals in most organizations that are working to address software security issues. The vast majority of information security practitioners have backgrounds in network operations, not software development.

Furthermore, they are often already spread thin resolving network security issues. At the same time, application developers have typically been rewarded for producing new features against tight deadlines, with little accountability for the security of the systems they build. In fact, rarely does any one person own responsibility for the security elements of the application itself. Development typically gets the business-critical application shipped, and the network operations team secures it. The dichotomy of these roles creates an extraordinary advantage for attackers – the only individuals truly experienced and focused on software security, or more precisely, software insecurity. Something needs to change. Security must be introduced into the software development lifecycle. The focus on perimeter security solutions looking in must become more balanced with software security solutions built from the inside out.

Software security – building it right the first time

What is required is nothing less than a fundamental change in the way we think about software development and information security – particularly for mission-critical business applications. Changes are needed in the way we specify, build, test, and deploy software: changes producing software that is robust, free of security vulnerabilities, and able to defend itself before it is compromised. This change will not come from simply proving that we have vulnerable code – we know that already. It comes from fixing code and, more importantly, fixing the process that creates these problems in the first place.

Software security goals must be achieved; however, they must be achievable without a wholesale departure from the way software is created or a significant impact on developer productivity. A balance must be maintained. Rather than spending large amounts of time and money on proving that we have security vulnerabilities after programs go into production, companies should go to the source and correct vulnerabilities as early as possible in the development stage. It is unquestionably faster, simpler, and cheaper for developers to correct vulnerabilities as they build programs.

But how can development management ensure that developers focus on security when there is no time or budget for security at the development stage? Even with the correct focus, how can they learn what to look for? How can they stay ahead of the dedicated and resourceful hacker? The answer is effective processes and better tools. With advanced software security tools, a developer can pinpoint vulnerabilities in a matter of seconds – the

same vulnerabilities that would take a hacker or manual code reviewer weeks or even months to find. These same tools can give development and information security managers useful metrics on application vulnerabilities before they are released into deployment.

The biggest impediment to this change is the prioritization of security as a critical requirement in our application development efforts. The best development managers work tirelessly to realize the requirements of their business users – they build what the business asks them to build. Until business owners set security as a fundamental software requirement, it is unrealistic to expect that change will just happen. It must start with the following management edict; The security of our business applications is a priority – software security is a fundamental requirement for new development efforts.

About the author: Roger Thornton is the CTO of Fortify Software, Inc. Fortify Software products protect companies from the threats posed by security flaws in business critical software applications. Its flagship software security suites for Source Code Analysis and Attack Simulation drive down costs and security risks by automating key processes of developing secure applications prior to deployment.. You can learn more about Fortify and its software security products by visiting www.fortifysoftware.com.

CHAPTER VOLUNTEERING OPPORTUNITIES

Chapter committees are always in need of people to lend a hand. Here are some opportunities available in various projects and events throughout the year.

The Web site Committee 249183 needs assistance in for the following projects. Please contact Dave McCandless at dave.mccandless@sfisaca.org for more information about Web site opportunities.

- Content gathering for the Chapter Web site. The work can be done from home, off hours, by e-mail or phone, and basically requires contacting people to gather chapter related information – chapter events, other chapter / international / other organization events we post, a listing of CPE events available to our chapter, job & employer listing, leadership team bios and pictures.
- Organization for the Chapter Web site. The Chapter Web site is in need of content organization into a structure that matches the hierarchy of the Web site.
- Content Conversion. Raw contend needs to be converted into from whatever format it arrives (word, excel, images, etc.) and need to be made in a "Web ready" format.

The Communications Committee needs volunteers for the following purposes. Please contact Mike Nelson at mnelson@securenet-technologies.com for more information about communication committee opportunities.

- Leverage their personal experience on interesting elements of the IT Audit function by writing an article for the newsletter.
- Provide an independent set of eyes to review (proofread) new newsletters before they go out.
- Join the team of people that will be reviewing and scoring the papers submitted to the Best Paper contest (evaluation period is May 17-31, 2005).

Information Systems Audit and Control Association

SAN FRANCISCO CHAPTER PRESENTS

2005 BEST PAPER CONTEST

FOR PROFESSIONALS AND STUDENTS

You write information on strategic and tactical IS audit issues, compliance concerns and audit methodologies.

Why not consider writing one that can potentially get you some extra cash and valuable recognition?

Key information	Awards	Selection Criteria	How to Participate
Application Submission Deadline February 16, 2005 **Entry Submission Deadline** May 16, 2005 **Contest Result** Announcement June 1, 2005 **Recognition** June 2005 (ISACA Luncheon Meeting) **Topics** Any topics related to information systems auditing (contact bpc@sfisaca.org to see if a topic you have in mind is acceptable)	**1st Place** $500.00 + Choice of free pass to the Fall Conference or a free pass to the CISA Review Course **2nd Place** $300.00 **3rd Place** $100.00 Winning papers may be published in the IS Audit & Control Journal and in the ISACA SF Chapter Web site and newsletter.	The best three papers will be selected to receive the awards. These papers must meet a certain minimum standards in order to be eligible. Please refer to the Review Criteria document for further details.	Download and fill out the application form and review criteria at www.sfisaca.org Questions regarding the contest should be addressed to: bpc@sfisaca.org

Buy a saver pass and save on training $$$

We would like to encourage members and non-members to participate in all Chapter Events and Seminars. As a way of encouraging participation, we are offering discounted rates for the advanced purchase of multiple education sessions. Saver Passes can be purchased in lots of ten for $300 and can be shared and are transfer able. Please check our Web site for more details.

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 christina.cheng@safeway.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, Mike Nelson at (925) 833-0286, or mnelson@securenet-technologies.com.

Save the date

The 5th Annual San Francisco ISACA Fall Conference will be held September 26th-28th, 2005, at the Hotel Nikko in San Francisco. The SF Fall Conference has established itself as the premier education event in Northern California for IS Audit and Security Professionals, and it is by far the best value. This three-day conference features four educational tracks, to accommodate different levels of experience and interests. More than 150 IS Audit and Security Professionals are expected to participate.

Random numbers

Did you notice some random six-digit numbers throughout this quarter's newsletter? Those aren't typos. They're ISACA membership numbers. Find yours somewhere in the newsletter and you win a prize! Just send a message to our Communications Committee Chair, Mike Nelson at mnelson@securenet-technologies.com and tell him you spotted your ISACA membership number in the newsletter. Good luck!

Learn about the San Francisco Chapter

Learn about the CISA certification

Learn about the CISM 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

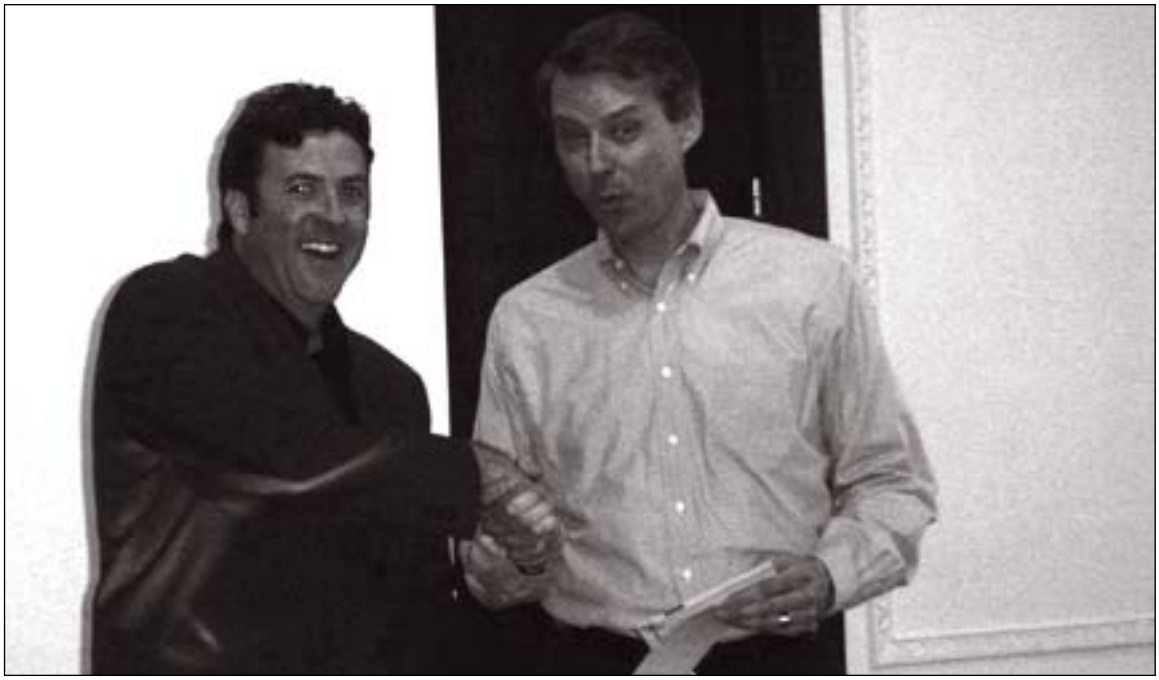
Contact Chapter Officers and Directors

ISACA AWARDS

Christina Cheng presents Donald Hester with his CISA pin

It was standing room only at the Fortify Software Presentation

ISACA AWARDS



Todd Weinman presents Dave McCandless with a Special Recognition Award

Education Committee Chair Bob Grill

SHOW YOUR DR/BCP (DISASTER RECOVERY/BUSINESS CONTINUITY PLANNING) KNOWLEDGE

Across

3. A sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property

5. The interruption of automated processing systems, support services or essential business operations that may result in the inability to operate

8. A predetermined plan for ensuring continuity of authority, decision-making & communication if key members of management become unavailable

12. Process of planning for and/or implementing procedures for the repair or relocation of the primary site and for the restoration of normal operations

13. _____ REVIEW A method of testing a component of a plan through a review for accuracy & completeness by someone with appropriate knowledge

15. Notification that a potential disaster situation exists or has occurred; direction to stand by for possible activation of appropriate plans

16. A predefined set of events and conditions that describe an interruption, disruption or disaster related to some aspect(s) of an organization's busines

18. _____ MIRRORING The duplication of data on separate disks in real time to ensure its continuous availability, currency and accuracy

20. The amount of work that accumulates when a system or process is unavailable

23. _____ REPLICATION Data replication or mirror in which the application is allowed to continue while the data is mirrored to another site

27. _____ WINDOW A period of time in which time sensitive business operations must be resumed

27. Process of planning for and/or implementing expanded operations to address time-sensitive business operations immediately following an interruption

30. The process of logging changes or updates to a database since the last full backup

32. A sudden, unplanned calamitous event that causes loss and hardship to all or part of an enterprise & significantly impacts its ability to operate

33. The process of planning for and/or implementing controls to avoid incidents & manage risks by decreasing the potential for incidents

36. An item of property and/or component of a business activity/process owned by an organization

37. The activation of the recovery organization in response to an emergency or disaster declaration

Down

1. _____ SITE An alternate site that contains physical space & building infrastructure to be provisioned at time of disaster

2. The reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required

4. The process of planning for and/or implementing the restarting of defined business operations following a disaster

6. The process of informing the recovery organization that an emergency exists in accordance with incident or emergency response procedures

7. The implementation of business continuity capabilities, procedures, activities, and plans in response to an emergency or disaster declaration

9. DATABASE _____ The partial or full duplication of data from a source database to one or more destination databases

10. A formal announcement by pre-authorized personnel that a disaster is predicted or has occurred and that triggers pre-arranged mitigating actions

11. _____ TEST A test conducted on one or more components of a plan under actual operating conditions

14. Potential for exposure to loss

17. An individual or company who provides a service(s) to a department or the organization as a whole

19. _____ EXERCISE A method used to test a disaster recovery plan to validate that information such as phone numbers, manuals, equipment is accurate

21. _____ SITE An operating location to be used when the primary facilities are inaccessible

22. _____ SITE A temporary location used to continue business functions after vacating a recovery site & before the original/new site can be occupied

24. Contract commitment that provides an organization with the right to utilize a vendor recovery facility for processing in the event of a disaster

25. A series of questions that relate to the various impacts of a business interruption or disaster

26. _____ AGREEMENT Agreement between 2 organizations with basically the same equipment/environment that allows each one to recover at the other's site

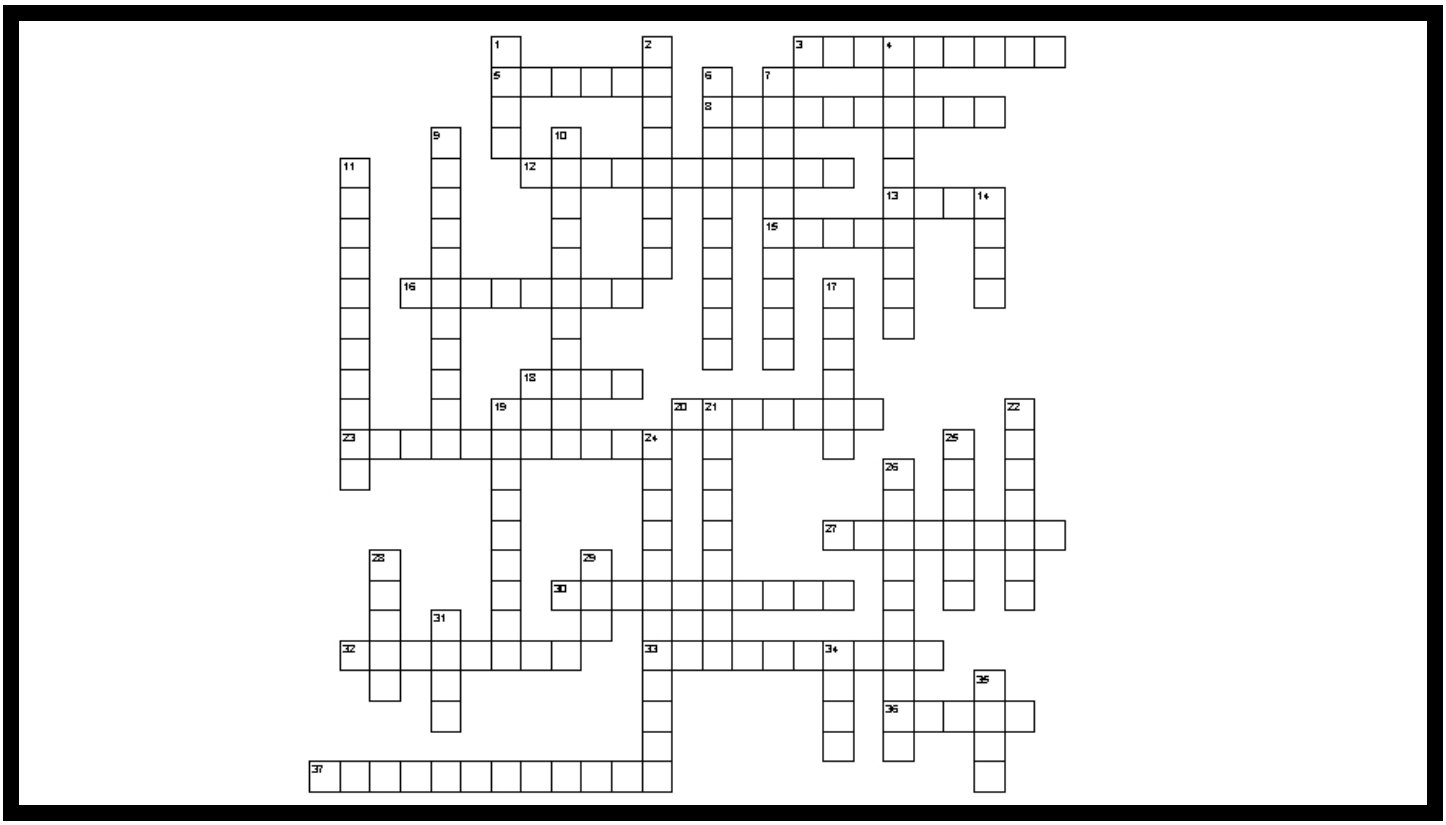
28. The process by which procedures and/or documentation are measured against pre-agreed standards

29. _____ SITE An alternate facility that has in place computer, telecomm & environmental infrastructure required to recover critical systems

31. _____ SITE A facility that is partially equipped with hardware, communications, power & air conditioning capable of providing operating support

34. An activity that is performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria

35. _____ CHECK One method of testing a specific component of a plan. Typically, the owner of the component reviews it for accuracy & sign offs



ACADEMIC RELATIONS

By Colin Lau – Academic Relations Committee Chair

Fall 2004 was a successful semester for the ISACA student chapter at San Francisco State University (SFSU). Through the leadership of Norma Rivera and Wendy Leung, not only was the student chapter able to pull off more events than in the past semesters, it has also increased its membership. I also want to express my gratitude to other officers for giving the required support to the chapter. These other officers I want to recognize are Sana Suleiman, Kiros Araya, and Jade Fang. The officers for the Spring semester were elected on November 30, 2004. Having first met the new chapter president at the 2004 SF ISACA Fall Conference at the Palace Hotel, I am looking forward to working with her and hope I can help her make the chapter more successful than ever. The last event the student chapter had for 2004 was the transition dinner held on December 22, 2004 and it was my honor to be invited. In the dinner I was given the chance to get acquainted with the new officers. Listening to their conversations about professors and classes, I felt I was still in school!

I am also working with Neha Suri from California State University – Hayward. Although there is no official student chapter in the Hayward campus, she is kind enough to offer personal assistance in promoting the Best Paper Contest for Students and the upcoming ISACA scholarship.

All in all, the San Francisco Chapter will continue to provide assistance to support the academic community. At the same time, the Academic Relations Committee will ensure a healthy relationship between our chapter and the student chapter.

MEMBERSHIP

By Beverly G. Davis, Membership Co-Chair

Members Make a Difference!

On behalf of the San Francisco Chapter Information Services Audit and Control Association, we welcome our new members and transfers from December 2004!

- M. Alilou Adamou, MCDBA, MCSE, CNA
- Nejat Aksoy, CISM, CISA, PMP
- Douglas A. Brown, CISM, CISSP, CCSA
- William Ek
- Amy L. Faubion, CISA, CBCP
- Sebastian Goodwin, CISSP, MCSE, CCNA
- Kenneth Hankoff
- Hanner Jane Hwa-Yih Shen
- Anthony Hargreaves
- Michel Kohon
- Satheesh R. Kumar
- Kent Lam
- Jasmin T. Limbo, CISA, CPA, CIA
- Claudia N. Lukas, CISSP
- Jeff Maze, MCSE, MCDST, CWNA
- Michael Smart
- Konstantinos Zafeiriadis
- David A. Eikel, CISA, CPA
- Darren C. Griffiths, CISA, CA, CIA
- Barry N. Gardin, CISA, CIA
- Anthony F. Ukena, CPA, CIA
- Frank Ping Kong, CISA, ABCP
- Lloyd Randall Lantz, CISM, CISA, CISSP, PFP
- Sugen Nadarajan Narainsamy, CISA
- Charles M. Neal, III, CISM, CISSP
- Kin Fai Cheung, CA, CIA

If you are interested in volunteering in support of the chapter please feel free to contact me at davisb@fhlbsf.com.

Thanks so much!

ASSET MANAGEMENT

by Andrew Ireland, Sr. Manager
Enterprise Risk Services, Deloitte & Touche LLP

IT Asset Management incorporates the acquisition, distribution, maintenance, support, replacement, reallocation and retirement of IT assets including all hardware and software utilized by an organization to achieve its operating objectives.

Many organizations attempt to manage all of these components using electronic management tools without any planning or consideration of their existing environment. 100812 In many cases important details such as cost, warranty, support, use and physical location are overlooked or ignored in the pursuit of short term gains to simply justify the money spent on the tool.

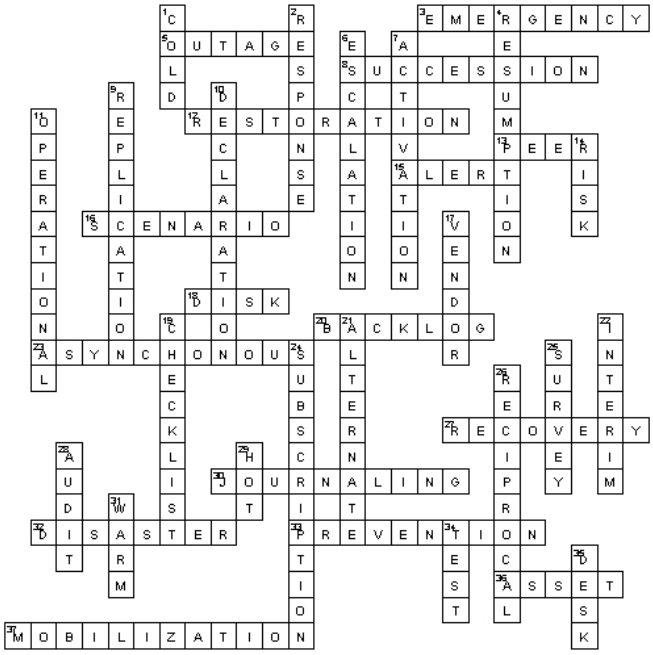
The recommended approach is to divide your IT asset management project into several separate initiatives capable of delivering savings both individually and as a whole. In many cases by merely addressing the deficiencies within your existing processes and procedures, immediate returns will be realized. For example: By defining budget responsibilities, comparing entitlements against deployment needs and establishing performance measurement criteria, an organization will be able to maximize volume purchase discounts, eliminate disparate off the shelf acquisitions and minimize the risk of costly non-compliance settlements in the event of an audit.

The following list of initiatives should be considered as part of any IT asset management program:

- Appointing an IT Asset Manager responsible for planning & budgeting, policy & procedure development, maintaining records and monitoring compliance,
- Planning and Budgeting that incorporates businesses objectives, existing resources, business needs and future opportunities,
- Development of Policies and Procedures governing the use of all IT assets from acquisition through retirement,
- Development of registers to capture all hardware and software related information including leasing terms, support contracts, product use and entitlement, agreement anniversaries, hardware and software interdependencies, reoccurring costs etc.
- Employee education on software acquisition, installation, piracy and use; and
- Self assessments to monitor compliance and identify opportunities to reallocate unused resources.

By phasing in the implementation of each of these steps, organizations will be able to save more money in the long run by having the flexibility to accommodate change over time both from a hardware point of view e.g. Wireless devices, PDAs, Smart Cards and from a software point of view e.g. Device, user, processor licensing, program changes and compliance reporting requests.

CROSSWORD PUZZLE ANSWERS



SAN FRANCISCO CHAPTER BOARD ROSTER 2004/2005

Executive Board

President
Lisa Corpuz
Providian Financial
(415) 278-4402
Lisa_Corpuz@providian.com

1st Vice President
Miguel (Mike) O. Villegas
Wells Fargo
(415) 243-5897
Miguel.O.Villegas@wellsfargo.com

2nd Vice President
Bob Grill
Wells Fargo
(415) 396-2919
Robert.L.Grill@wellsfargo.com

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

Treasurer
Heidi Yu
Federal Reserve Bank of SF
(415) 977-3930
heidi.yu@sf.frb.org

Past President
Christina Cheng
Deloitte & Touche
(408) 704-4203
chricheng@deloitte.com

Directors

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

Kevin Fried
Deloitte & Touche
(415) 783-4639
Kefried@deloitte.com

David McCandless
McCandless Systems
(925) 938-6508
dmm@mccandless.com

Mike Nelson
SecureNet Technologies, Inc.
(866) 660-0249
mnelson@securenet-technologies.com

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

Jimmy Yip
Ernst & Young
(415) 951-1536
Jimmy.Yip@ey.com

Justin Gibson
KPMG LLP
(415) 951-7219
justingibson@kpmg.com

Committees

Academic Relations
Colin Lau

CISA Review
Conny Cheng

CISM Review
Christina Cheng, coordinator

Communications
Mike Nelson, Chair
David McCandless, Web master

Membership
Christina Cheng, Co-chair
Beverly Davis, Co-chair

Volunteer
Brian Alfaro

Education
Bob Grill, Co-chair
Jimmy Yip, Co-chair

Fall Conference
Anna Chan
Beverly Davis
Bora Turan
Clyde Valdez
Colin Lau
Danielle Laversin
Dave McCandless
Justin Gibson
Kevin Fried
Lisa Corpuz
Michele Ling
Mike Nelson
Mike Villegas
Nejat Aksoy
Todd Weinman

Advisory Board

Advisory Board
Robert Abbott
Kathryn Dodds
Chuck Dormann
Doug Feil
Carol Hopkins
Roberta Hunter
Edmund Lam
Dave Lufkin
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