

OFFICERS AND DIRECTORS 2002-2003

PRESIDENT

Carrie Schrader, CISA, CBM
Handleman Company
248-362-4400 ext. 358

VICE PRESIDENT

Mike Stolarczyk, CISA
Jefferson Wells International
248-350-3006

TREASURER

John McCormick, CISA, CIA
The Detroit Medical Center
313-966-5104

SECRETARY

James Cramer, CISA
The Detroit Medical Center
313-966-5170

DIRECTORS

Salman Aziz
The Detroit Medical Center
313-966-5155

Ed Barszcz, CIA, CFE
Blue Cross/Blue Shield of MI
313-225-9076

Gerald Baumgart, CISA
Comerica
248-371-7060

Patti Earl-Cole, CISA, CIA
Blue Cross/Blue Shield of MI
313-225-8577

John Hoppesch, CISA
Kmart Corporation
248-614-9975

Brenda Karl, CISA
Jefferson Wells International
248-350-3006

Michael Mullens, CISA, CIA
General Motors
cell 586-382-1543

Brandy Pfeiffer, CPA
Federal-Mogul Corp
248-354-2602

John Quaine II, CISA, CPA, CIA
Blue Cross/Blue Shield of MI
313-225-7663

Cyndi Shelton, CISA
General Motors
734-604-1797 cell

David F. Thompson, CISA
Blue Cross/Blue Shield of MI
313-225-6384

Sander Wechsler, CISA, CPA
cell 313-492-6071

Karine Wegrzynowicz, CISA
Ford Motor Company
313-337-5796

PAST PRESIDENTS

Art Abruzzo, CISA, CDP, CSP
Amerisure Companies
(248)-426-7944



*Information Systems
Audit and Control
Association*

DATABYTE

NEWSLETTER OF THE DETROIT AREA CHAPTER

VOLUME 17, #3

REGION 2, CHAPTER 8

NOVEMBER, 2002

Monthly Meeting

Wednesday, November 20, 2002

Pre-Dinner Topic: "Auditing Servers"

After-Dinner Topic: "Auditing Servers"...continued

**Location: Big Fish Seafood Bistro
1111 W. 14 Mile, Madison Heights
Corner of 14 Mile/ Stephenson Hwy.
248-585-5933**

Date: Wednesday, November 20, 2002

**Time: 4:30-5:00 Registration/Networking
5:00-6:00 Before-Dinner Presentation
6:00-7:00 Dinner
7:00-8:00 After-Dinner Presentation**

**Cost: \$30.00 Members
\$35.00 Others
\$20.00 Students and Retirees**

Reservations will be taken by John Hoppesch. If possible, please make reservations by 4:00 pm Friday, November 15, 2002. You can make your reservation online at isaca-det.org or e-mail your reservation to John Hoppesch at jhoppesch@yahoo.com. If you do not have access to the Internet, call John Hoppesch at 248-672-4076 or fax your reservation to him at 248-614-0701. Please include your name, company, telephone number, and whether you are a Member, Non-member, Student or Retiree. Walk-ins are welcome, but the food selection may be limited.

Visit our web site at: isaca-det.org

Letter from the President

Dear Members,

I hope that everyone enjoyed the excellent presentations at the October dinner meeting. I would like to thank Mr. Sadaghiyani from Blue Cross Blue Shield of Michigan not only for a wonderful and informative presentation, but for providing the group with a handout that can help all of us identify security concerns in the Oracle environment. Additionally, I would like to thank Mr. Layne from Avotus Corporation for giving us a look at some new tools to be used in the telecommunications area, which provide monitoring of e-mail and internet usage as well as schematic mapping of the telecommunication networks. Both speakers are making their presentations available to us to post on our website. Please watch the website at www.isaca-det.org for these new additions.

This month we have planned an educational topic “Auditing Windows Servers“. The topic will be split over our pre-dinner and after-dinner sessions. Be sure to arrive early to take advantage of the entire presentation. As a reminder, you can register through our website by selecting “Register for Next Meeting” from the home page.

As promised in the first issue, I would like to take a moment to give you some background on one of our committees. This month I would like to focus on the Membership Committee. The chairperson for this committee is Brenda Karl. She and several board members coordinate three aspects of the Membership Committee, including membership, student relations and job bank. The committee is responsible for:

- Encouraging and improving over-all attendance at ISACA Chapter meetings through membership campaign programs, as well as, networking with other companies and organizations. Additionally, they survey reasons for absences and work to correct any identified shortcomings.
- Promoting interest of prospective members and maintaining the interest of current members.
- Communicating all local and International ISACA programs to the Chapter’s membership.
- Surveying members and non-members annually to ensure the Chapter is meeting the needs of it’s members and prospective members.
- Ensuring that membership profile changes are communicated to International and verifying that updates made are appropriate.
- Networking with local colleges and universities to

- promote the IT audit profession and the organization.
- Maintaining and updating the Chapter’s job bank to communicate available positions to our membership. If you would like to become involved with the programs committee, either now or in the future, I encourage you to contact Brenda or myself for further information.

As always, the board is here to serve the membership. If you have any suggestions on how to improve any of the programs that we offer or to provide ideas for new programs, please contact Mike Stolarczyk, myself, or any of the board members listed on the front page of this newsletter. We would be happy to help and look forward to hearing from you.

Carrie Schrader
Chapter President

AUDITING SERVERS

Dean Therriault – Bio
MCSE, MCT, A+, Net+

Dean is a Microsoft Certified Instructor specializing in technical education. His main disciplines lie with the Microsoft NOS’s. As a Microsoft Certified Systems Engineer, Dean has demonstrated his proficiency, and ability to plan, configure, deploy, and maintain solutions implemented on Microsoft platforms.

Dean’s main area of expertise is in the classroom teaching Windows 2000 related courses. These range from entry level Windows 2000 Professional training for the help desk, to more advanced Active Directory design and implementation courses targeted at high level IT professionals.

Security is an ongoing concern and should never be viewed as complete. It’s important to note that Dean has considerable experience in the production environment. Routing and remote access, Web servers, and Terminal servers are among the types of systems Dean routinely secures. IPsec, SSL, PPTP, L2TP, and Packet filtering are technologies frequently implemented when security is vital. When addressing network and system security nothing is taken for granted. Dean approaches all security issues with vigilance to ensure that every possible backdoor is secured and accessible only by authorized users.

It’s no secret that the real world is much different than the classroom and Dean uses his real world experiences to bridge the gap between the real world and the classroom.

CISM, the Certified Information Security Manager is ISACA's new certification and is specifically geared toward experienced information security professionals. CISM is business-oriented and focused on information risk management while addressing management, design and technical security issues at the conceptual level. 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. The Detroit Chapter ISACA board will bring you more information as it becomes available; however, you may access the ISACA International website at www.isaca.org/cert1.htm for the information that is currently available.

ISACA announces the 2003 Certified Information Systems Auditor Examination on June 14th 2003.

The only globally recognized certification program for information systems audit, control and security professionals announces it's next examination. For the 22nd consecutive year ISACA will administer the Certified Information Systems Auditor (CISA) Examination. The 2003 CISA Examination will be conducted on Saturday, June 14, 2003, and will be offered at more than 180 international test centers in 58 countries. The exam composed of 200 multiple choice questions, will be held in one four-hour session. The 2003 CISA Examination will be offered in ten languages.

The exam covers the following process and content areas: 1) The IS Audit Process; 2) Management, Planning and Organization of IS; 3) Technical Infrastructure and Operational Practices; 4) Protection of Information Assets; 5) Disaster Recovery and Business Continuity; 6) Business Application System Development, Acquisition, Implementation and Maintenance; 7) Business Process Evaluation and Risk Management.

This international certification program grants the title of Certified Information Systems Auditor (CISA) to candidates who achieve a passing score on the examination and demonstrate five or more years experience in the information systems auditing, security, or control professions.

The CISA designation is widely recognized as a professional standard of excellence. More than 23,000 specialists in Information Systems Auditing Security and Control have earned the designation worldwide.

A Candidates Guide to the CISA Examination, the 2003 CISA Review Technical Information Manual, the 2003 CISA Review Questions, Answers and Explanations Manual, the CISA Review Questions, Answers and Explanations 2003 Supplement and the CISA Review Questions, Answers and Explanations CD_ROM are available from ISACA to help candidates prepare for the exam. Detailed information can be obtained from ISACA by phone at 1.847.253.1545, Certification Department, by fax at 1.847.253.1443, or by e-mail at certification@isaca.org.

The Detroit Chapter will once again offer a CISA Examination Review Course. Please watch future issues of the Databyte and website, www.isaca-det.org for further details.

NEW CHAPTER MEMBERS

New Chapter Members for August

- * Mark Henry
- * Shannon Herbst
- * Amine Houari
- * Shruthi Kuiper
- * Rajesh Nayak
- * Ronald Pioch
- * Sukanya Rangarajan
- * Gail Ricketts
- * Linda Scibilia
- * Michael Stokes

Incoming Member Transfers for August

- * David Foy
- * Kunle Coker

New Chapter Members for September

- * Jonathan Nobis
- * Daniel Shoemaker

Incoming Member Transfers for September

- * Shelby Craddock

AUDITING FOR PROFIT

By Gordon Smith
President, Canaudit Inc.

Every day we are bombarded with more bad news about American corporations. Profits are vaporizing, staff is being laid off, businesses are going bankrupt, and entire product lines are shutting down. While everyone is saying how bad things are and asking where the bottom is, I take a contrarian view. This is the best time to be an internal auditor. The internal auditor is one of the few accounting professionals that have not been tarnished by recent events. So much so, that many organizations are asking the internal auditors to scrutinize the work of the external auditors.

As the deadline approached for CEOs and CFOs to certify the financial statements of many U.S. corporations, the internal auditors diligently reviewed the numbers, asked the right questions, and provided management with the answers they needed. Should we certify or restate? As the deadline passed, we saw that many companies were able to certify their statements. Meanwhile, other corporations decided to restate their earnings, many of them taking significant hits on the

stock price. I can only imagine the work that led to these restatements and the debate of the issues prior to the restatement. I'm sure that we will see other restatements in the near future as more corporations hit their deadlines or more issues come to light from the additional scrutiny of internal auditors.

With that said, given the cleansing of balance sheets, many organizations have had earnings shortfalls. These companies need internal auditors to help them find new areas for profit enhancement. About a decade ago, I wrote a Cnaudit course called Auditing for Profit. In this course, we demonstrated how internal auditors could use a financial statement review to target capitol and labor inefficiencies, thereby increasing earnings per share. Using these analyses, they could target their audits to maximize return and provide management with suggestions to enhance profits and cash flow. The areas we focused on were escalating payment of receivables, stretching receivables, increasing inventory turns, and releasing surplus real estate. In preparing to rewrite this course, I realized that auditing for profit must focus on several other issues as well.

Executive Compensation vs. Executive Performance

Forbes magazine did an excellent study of the best-paid CEOs. The following URL is a great place to start: <http://www.forbes.com/2002/04/25/ceos.html>. Mr. Eisner won the prize for the worst CEO (<http://www.forbes.com/forbes/2002/0513/112tab.html>). In the last five years, his compensation was in the \$750 million range. Yet last year, Disney laid off 4,000 employees. Meanwhile, Mr. Carty of AMR coproraiton received a compensation package of \$3.8 million last year; yet, they recently announced that they would lay off 7,000 people. Mr. Carty has to make tough calls; however, his package is nowhere near Mr. Eisner's. In my mind, it is a simple matter to determine which CEO is properly paid to make the difficult decisions. The questions I must ask of Disney, as an auditor, are could \$700 million, diverted from executive salary to marketing or product development, have saved some or all of those jobs and enhanced revenues? Would the money have been better spent if it were returned to the shareholders in the form of dividends? Would the stock price be higher today if one or all of these alternatives had been implemented? The press and the stock analysts

are also asking these questions. Now, several General Auditors are being asked to add executive compensation to the list of audits they perform. I say it is about time! What better way to find additional profit than to ensure that executives are properly paid, based on their performance.

Now, I am not saying that executives should be paid less. I agree with Forbes Magazine: executives who provide a good return to shareholders while enhancing shareholder value should be rewarded. Mr. Golisano of Paychex was rated the best CEO of 2001 because of the value he provided to the company and the \$800,000 package he received last year. Mr. Golisano deserves to be rewarded and be well rewarded. If I were the General Auditor of Paychex, I would have to recommend that his compensation be increased. If, on the other hand, I were General Auditor of Disney, I would have to recommend to the compensation committee that Mr. Eisner's package be reduced or, given his poor performance, that he be terminated. That would definitely be a career limiting move, but every once in a while we are called upon to make the difficult decisions, even at the cost of our position. As the General Auditor for American Airlines, I would suggest that Carty is properly paid.

I suspect that many auditors will shy away from the executive compensation issue. That is their choice and I respect them for making it. There are other auditors who will jump at this assignment. Yes, it is politically risky; however, it is a tough job and someone has to do it. I think internal auditors can be independent and fair. They know that if an executive is overpaid, then the shareholders and employees are not happy campers. Conversely, the internal auditors know that if you underpay a key executive, then they risk losing the executive. The members of the compensation committee of the Board of Directors will respect the auditors analysis and give it due consideration along with other factors in setting executive compensation packages. Therefore, to those of you who are willing to rise to this challenge, I say, "audit the compensation packages". It will require a significant effort; however, in the end, it will be a very interesting and rewarding audit. The outcome will also have a significant impact on the profits of the corporation.

Auditing Corporate Downsizing Plans

Imagine how employees must feel when they find out that they are being laid off; yet, the company bought an \$18 million dollar apartment for the CEO. Consider this scenario. You are a dedicated, loyal employee of 15 years with highly regarded skills. Your company announces a large layoff of white-collar staff. What are you going to do the next time a headhunter calls about another job? What if the new job includes a 10% pay increase and incentive programs tied to your performance? One of the greatest risks in any downsizing program is the chance that you could lose your best employees because they are uncertain of their future. Those who can leave for a better job may very well leave. That reduces the number of staff that need to be laid off, so management may say they are achieving their objective.

However, consider this: If the company is downsizing and it loses the cream of the crop, what are they left with? The average performer, if they stay, will provide value, but what happens when those who are left are so poorly skilled that they cannot get a job elsewhere? Where will the under-performers go? I say they will stay with the organization, cling to their jobs, keep a low profile, and, if they are lucky, miss the staff cuts. When this happens, the corporation is left with the cream of the crap! The under-performers cling together to save their jobs, while the cream of the crop is now assisting their new employers to achieve higher profits and expand market share. The corporate intelligence deteriorates. Over time, this will accelerate the poor performance of the organization and create a downward spiral that could end in bankruptcy.

My new version of auditing for profit addresses this issue. Internal Audit must review corporate downsizing plans. Not only must they identify unfair or discriminatory practices in the downsizing decisions, but they must ensure that the correct people are designated as surplus. If there is an under-performing executive with a \$2,000,000 compensation package, should we let this person go or lay off a 100 \$20,000 per year factory workers? We will need revenue to enhance profits. Will 100 workers be able to turn out more product, so that the company can increase sales

and hence profits? If so, then I say get rid of the executive and keep most or all of the workers. Conversely, if product sales will not be increased, and there is a long-term negative shift in the demand pattern, I say let the workers go, as well as the under-performing executive.

When I hear calls for a 10% across the board reduction in workforce, I cringe. Does this mean that all departments will have to cut by 10%? Is that 10% of the head count, or 10% of the payroll value. Letting one or two under-performing executives go, could save enough money to keep production up. Remember, we need people to produce product, whether the product is widgets or consulting services.

Another point to consider in the downsizing is the amount of work that is done and who does it. Some of you who have been in my classes will remember Gordie's three laws. The first is that work flows to the lowest level willing to accept it. Who does more real backbreaking work: the welder in the plant or the Manufacturing Vice President?

The second law relates to information security. This law states that the rule of least access becomes the rule of most access, because of Gordie's first law. As companies threaten layoffs, the security risk increases. The teller has more access to customer information than the CEO. As a result, the teller could sell information to competitors (bank balances, names, addresses, social security numbers, etc). Clearly, the tellers have far more access to data than others in the bank; yet, they are poorly paid and subject to constant downsizing as automation eliminates their positions.

Gordie's third law states that the amount you are paid is inversely related to the amount of work you do. Who gets paid more, the bank CEO or the teller? Whose feet are aching at the end of the day, the CEO's or the teller's?

Based on the third law, it makes sense to me to identify the layers of managers who are very well paid, but not really providing value. Throughout my career, I always wondered how managers could waste so much time in meetings; yet, achieve little or nothing. I reviewed the meeting calendars for several clients and found that

many people spend more than 80% of their time in meetings. In many cases, the meetings have far more people in them than required. I have watched some of these people sit like lumps on a log, providing no input to others in the meeting. Why are they there? Well, if they are not present, they may get bad mouthed by others or saddled with additional projects. Politics being what it is, it is best for people to be present in a meeting even though they are not required rather than risk the political danger of being absent.

I have several solutions to this. The first is to identify those managers and staff who will be in a meeting. Next, take the hourly salary for each person and add this up. This provides the hourly cost of the meeting. For each manager in a given meeting, let's assume that their salary is \$100,000 and the fringe package costs about \$30,000. That means their annual costs are \$130,000 per year. Now let's assume each gets three weeks vacation and one week of personal / sick time per year. This results in the potential for 48 weeks of productive time. Simply dividing the salary plus fringe by the number of weeks available for work and the normal number of hours in a workweek, we have an approximate cost of \$68 per hour.

Now let's assume that the average staff member in a meeting gets a salary of \$70,000 per year and the same fringe package of 30%. That gives us an approximate price of \$47 per hour, per person.

If a given meeting has three managers and four staff, our hourly cost for the managers and staff is \$392. Assuming there are two consultants in the meeting with an hourly cost of \$300, including expenses, the meeting has a cost of \$992 per hour, which we round to \$1,000 per hour. If the meeting lasts three hours, it costs the company \$3,000. This is just a small meeting. As the number of people in the meeting expands, then the cost of the meeting also increases. In a given company, there could be 20 such meetings a day, resulting in a cost of \$60,000 per day. How many widgets do we have to sell to recover the \$60,000?

Posting the meeting cost in the room and the accumulated cost of the meeting as it progresses, will help the participants realize the cost of the meeting, and may help them stay focused. The next step is to track the number of items discussed by outcome. Each item

discussed could have several outcomes. Items could be resolved, they could be tabled for another meeting, or they could be passed to another group for discussion and resolution. Most items discussed should be resolved with a clear decision arising from the discussions. Unfortunately, this does not happen as often as one would like. Normally, items are discussed ad nauseum, and then tabled when no consensus can be reached. As a result, the people in the meeting decide to meet again. This is a welcome outcome for the consultants; however, it just increases the organization's overhead.

Clearly, meetings need to be managed, the costs of meetings tracked, and the participant list whittled down to those who are absolutely necessary.

Now some of you may say that we cannot predict exactly who should be in the meeting. Therefore, we need to invite those who may have a need to be there. This leads me to another way to save costs. If someone may be needed for a meeting, put him or her on notice that they may be called. Then, use the speakerphone in the meeting room to call them if necessary. They can listen in to their part of the meeting, then return to other tasks after they provide the information required or assist in the decision making process.

Several of my clients are making effective use of intranet web casting and chat programs to bring people together to discuss ideas. With good management, this reduces the cost of the meeting by eliminating travel time and enabling people to join the meeting as required. The moderator of the meeting invites people and also uninvites them at any time.

Reducing time wasted in meetings will result in enhanced productivity; yet, still enable the right people to be present in a meeting for the period of time when they are needed.

Now, how do meetings tie into selecting people for downsizing? In my many years as an auditor, I have noticed that some managers spend most of their time in meetings rather than managing their staff. Therefore, I developed a fourth law. Gordie's fourth law says that if a manager spends more than 60% of their time in meetings, then they are not managing their staff. They should be candidates for downsizing. After all, when

the boss is away, the staff may play. A manager's job is to manage, not sit in meetings when there are more important items to be performed.

Now let's tie the propensity to waste time in meetings to the requirement to downsize. Why not review the electronic schedules of all managers to identify those who spend more than 60% of their time in meetings? Let us determine if they are being effective or not, and if there are some who should go. I say that some of these managers could be safely terminated. To ensure we do this right, let us review the minutes of the meetings to see if the meeting objectives were met, who contributed effectively, and those who simply kept a chair warm.

Since I also believe that the layers of corporate management are bloated, letting a number of managers go not only would enhance communication lines and flatten the structure, it would force managers to become managers!

Cutting the Politics, Getting Results

In many organizations that I visit, I find politics are rampant. Managers often want to make the politically correct move rather than the best decision for the company. In some organizations, peers seem to be more like piranha fish than teammates. If one person makes a mistake, one or more of the other team members may use the mistake for their political gain even though the company gains little of nothing.

In some companies, the politics not only increases the costs of doing business, but may result in the loss of some of your best people. Therefore, when you notice political rather than business decisions are being made, ask those assembled if the decision is the best one for the company as a whole. I find that by constantly asking this question, better decisions are made.

The Last Gem in this Article

I like to save the best ideas to the end. If you are still reading this article, then I certainly need to reward you. Here is my best money-saving idea. About once a year at Canaudit, we have our staff record everything they do. This enables us to identify processes that are no

longer required, staff that are over-burdened, and procedures that impede our ability to serve our customers. We give this data careful consideration and, surprisingly, many good ideas are a direct result of our own review.

The first question I ask when I am doing operational audits or audits for profit is: why is the client doing what they are now doing? The second question is: what value does this add to the corporation? It is surprising the number of tasks we identify that are a complete waste of time and add no value. I will save actual examples for the new class. Now that you know the questions to ask, why not ask them before coming to the course? Let us get rid of useless processes, dead wood in management, and release assets that are not providing value. Let us do it now, so that we can give the shareholders the value they deserve for maintaining their investments in these difficult times.

There are more items to be covered here, but we have to leave something for the auditing for profit class. It will be premiering in 2003 at a chapter near you. If it is not offered in your area, we will be offering it in Simi Valley and Washington DC several times in 2003.

As always, the comments in this article are mine alone. I expect that some of the items will cause debate and I encourage the debate. For companies to become more profitable, we have to consider new ideas, many of which may seem radical. All I ask is that you read the article, ponder my comments, and think about the issues. Please feel free to email your comments to me via gordon@canaudit.com. I value your opinions and will personally respond to each comment.

If you would like to meet with me to discuss any of these issues, I will be available during the IT Audit Boot Camp and Ultimate Network Penetration Course in the Washington, DC area. I look forward to seeing you there.

Gordon Smith

Gordon Smith
President,
Canaudit Inc.

The Year At A Glance

November 20, 2002
December 11, 2002 (IIA)
January 9, 2003 (CFE)
February 19, 2003
March 19, 2003
April 16, 2003
May 21, 2003

Auditing Servers
Computer Incident Response Team
No presentation at this time
CISA/CISM Roundtable
To be determined
Risk Analysis/Audit Planning
Auditing Windows 2000

Auditing Servers cont.
Technology Update
To be determined by CFE's
Virus Protection
To be determined
Single Sign-on Solution
E-Business System Development

The 4th Annual Spring Conference dates for 2003 have been set. They are March 24, 25 and 26, 2003.
(Co-sponsored by the Detroit Chapter of the IIA and Detroit Area Chapter of ISACA)

Menu - November 20, 2002

When making your reservation, please indicate which entree you prefer. Attendees not specifying a choice will be served entree #2.

The following entrees will be served:

Entree #1 N.Y. Strip Steak
Entree #2 Rosemary Chicken (Cream Garlic Sauce)
Entree #3 Broiled Whitefish

A vegetarian plate is available for those on special diets.



All meals include:

- Specialty Bread
- Rice or Potato of the Day
- Tossed Salad with Raspberry Dressing
- Fresh Seasonal Vegetable
- Dessert: N.Y. Style Cheesecake
- Coffee or Tea
- Cash Bar Available

The Chapter must provide the number of reservations by the Monday before the meeting. To ensure that we can accommodate those who wish to attend and the restaurant can provide the best service possible, please make your reservations early. If you have made a reservation and cannot attend, please call John Hoppesch at (248) 672-4076. Your cooperation is greatly appreciated.

Monthly Drawing Winners!!

Art Abruzzo - Amerisure
Patti Earl-Cole - BCBSM
Samantha Ngo - Walsh College Student
Mario Pennesi - Green Shield Canada

DATA BYTE

DETROIT AREA CHAPTER
P.O. BOX 4297
TROY, MICHIGAN 48069-4297

*Information Systems
Audit and Control
Association*

