

ICON

ISACA CENTRAL OHIO NEWSLETTER

Volume 11, Issue 6

February 2000

Meeting News

DATE: Tuesday, Feb. 8, 2000
Joint IIA/ISACA Meeting

AGENDA: 11:15 Registration
11:30 Lunch
12:15 Organizational Business
12:30 Speaker

LOCATION: Buckeye Hall of Fame Café
1421 Olentangy River Rd.
Columbus, OH 43212
(614) 291-2233

★ Directions on Newsletter Cover ★

MENU: Hot Luncheon Buffet:
Mixed Greens with Assorted Dressings,
Pasta Salad, Fresh Fruit Display with
Dip, Cottage Cheese with Peaches,
Roast Sirloin Bordelaise, Creole
Chicken, Garlic Smashed Potatoes,
Steamed Vegetables, Rolls and Butter,
Coffee, Hot Tea & Iced Tea,
Array of Desserts

PRICES: \$ 15.00 Members
\$ 18.00 Non-Members
\$ 5.00 Student (Student is full-
time undergraduate, non-
professionally employed)

RSVP: Richard Ridewood 466-4083
Fax: 728-7199
e-mail: rridewood@auditor.state.oh.us

RESERVATIONS POLICY

The deadline for reservations is **Friday, Feb. 4, 12:00 noon**. If you do not reach Rich directly, please be sure to leave the following information: Name, Member/Non-Member, and Company. **Cancellation deadline is Friday, Feb. 4, 12:00 noon. Names can be added, but cancellations must be made by the cancellation deadline.**

ALL RESERVATIONS MADE AND NOT CANCELED BY THE DEADLINE MUST BE PAID FOR.

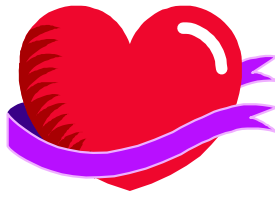
Electronic Data Management

Nelia Pozzuoli - Computer Risk Manager - Electronic Data Management. Nelia has over 18 years experience as an Information Technology Auditor in a variety of industries including automotive manufacturing and software development firms. Relevant experience includes:

- Designing, developing and executing Electronic Data Management solutions in a variety of industries, including a 1.5 billion automotive software development firm.
- Performing open systems security evaluations at a 1.5 billion automotive software development firm Performing Project Management Assessment and ERP
- Post-Implementation review at a 3 billion multi-national business systems supply firm including on-site review of three foreign subsidiaries. This project included use of Electronic Data Management techniques to perform revenue assurance for the Company's German and French subsidiaries.

Inside This Issue:

Chapter Directory & Agenda	p. 2
President's Message	p. 3
Education Updates	p. 3
Conference Updates	p. 3
Monthly Article	p. 4-5
Directions	p.6



**DIRECTORY OF OFFICERS, COMMITTEE
CHAIRPERSONS, & DIRECTORS
1999 - 2000 CHAPTER YEAR**

OFFICERS:

President: Norman Hofmann, (614) 728-7164
Ohio Auditor of State

V-Pres: Ken Kuss
Nationwide Ins.

Secretary: Jim D'Innocenzo, (614) 466-4085
Ohio Auditor of State

Treasurer: Tim Winslow, (614) 213-6336
Bank One Corporation

COMMITTEE CHAIRPERSONS:

Arrangements: Richard Ridewood, (614)466-4083
Ohio Auditor of State

Audit: Greg Mason, (614) 728-0125
MRDD

Education: Richard Ridewood, (614)466-4083
Ohio Auditor of State

Membership: Jim D'Innocenzo, (614)466-4085
Ohio Auditor of State

Newsletter: Tamela Bolte, (614) 728-7117
Ohio Auditor of State

Programs: Ed Bell, (614) 331-9355
Huntington Bancshares, Inc.

Norman Hofmann, (614) 728-7164
Ohio Auditor of State

DIRECTORS:

Ed Bell, Huntington Bancshares, Inc. (614) 331-9355

Richard Ridewood, Auditor of State (614) 466-4083

Brian O'Brien, OSU

Claudia Mitchell, Nationwide Ins. (614) 249-4110

Allison Williams, Nationwide Ins.

Larry Frazee, Huntington Bancshares, (614) 480-6525

Mike Jenkins, CBSI, (614) 220-4411

MEETING DATES

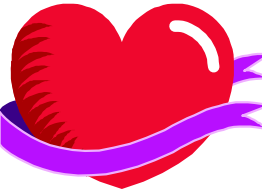
2/8/00	Joint meeting with IIA Buckeye Hall of Fame
3/2/00	Monitoring and Intrusion Detection
4/6/00	TBA
5/11/00	TBA

**ISACA CENTRAL OHIO CHAPTER
DISCLAIMER STATEMENT**

Because it is one objective of the ISACA Central Ohio Chapter to be a forum for the free expression and interchange of ideas, statements of position or expression of opinion appearing herein are those of the author(s) and not by the fact of publication necessarily those of the ISACA Central Ohio Chapter. Likewise, the publication of any advertisement in the ISACA Central Ohio Chapter's newsletter is not to be construed as an endorsement of the product or service offered unless such approval or endorsement is specifically stated.

ICON: ISACA Central Ohio Newsletter is published monthly. Articles and advertisements are welcome. The deadline for receiving articles is the 10th of the month prior to the month the article is to be published. Current advertising rates: \$30 for full page and \$20 for half page. For further information contact:

**EDITOR: Tamela Shreve-Bolte
Ohio Auditor of State
35 East Gay Street
Columbus, OH 43271-0386
PHONE: (614) 995-4834
FAX: (614) 728-7199
E-MAIL:
tjbolte@auditor.state.oh.us**



**PRESIDENT'S MESSAGE:
From the Desk of Norman Hofmann**

I would like to thank Rich Ridewood for his informative presentation on using ACL to review AS 400 systems. Our January meeting was well attended and I think everyone gained a few insights from the presentation and enjoyed the food. This month's meeting is our annual joint meeting with the local IIA chapter. The speaker, Nelia Pozzuoli, is an experienced EDP auditor and a past president of the Cincinnati ISACA chapter. Her topic of ERP and its relationship to E-commerce should be of interest to all of us. ***This month's meeting will be on Tuesday February 8th at the Buckeye Hall of Fame Cafe.***



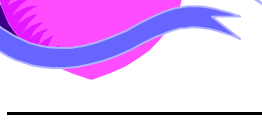
Our program for the rest of the year is almost complete and promises to be both entertaining and educational. The chapter will be offering a spring seminar in partnership with ISSA. The seminar will be on April 26th - 27th, which is a Wednesday and Thursday. The seminar is from the MIS Training Institute and is entitled ***The Good Guys' Guide to Testing Network Vulnerability: Pinpointing and Probing Systems Exposures.*** The speaker will be Mr. Ken Cutler, who is one of their top presenters. More details will be provided in subsequent announcements.



- Other dates of Interest:
- IS Audit and Control Training Week, 13-17 March 2000; Philadelphia, Pennsylvania**
 - 17-21 July 2000; Orlando, Florida**
 - North America CACS 2000, 7-11 May 2000; Dallas, Texas**
 - International Conference 2000, 16-19 July 2000; Lake Buena Vista, Florida**
 - Network Security Conference, 21-23 August 2000; Las Vegas, Nevada**
 - eBusiness Conference, 21-23 August 2000; Las Vegas, Nevada (Tentative)**



The final registration date for the 2000 CISA exam on June 10, 2000 is April 3, 2000. To date, I have had only a few responses expressing interest in a CISA review class. Anyone interested in a review class should contact either myself or Ed Bell.



A reminder to everyone that this newsletter is available in a PDF format. A copy of each month's newsletter will be posted on our chapter Website, www.osu.edu/units/uts/isaca-centralohio/, on approximately the 20th of each month. In addition, we

will Email a PDF copy of the newsletter to all members who would like to receive a copy in that format. Just contact either myself or the chapter newsletter co-ordinator if you would like to receive your newsletter this way.

Remember, due to the breakeven nature of our meeting budget for this year, reservations made but not canceled before the deadline ***will*** be billed for.

There will be a board meeting at 10:30 before this month's chapter meeting.

**Network Security Conference
21-23 August 2000; Las Vegas, Nevada**

ISACA is pleased to announce the 2nd annual Network Security Conference. Building on the overwhelming success of the first conference, the second will feature longer and more focused presentations. Keep watching the ISACA web site in 2000 for details.
www.isaca.org/conf1.htm

Education

Another valuable educational opportunity is on the horizon. So mark your calendar for April 26/27, 2000 for another ISSA/ISACA Joint Seminar. The instructor will be Ken Cutler, "The Good Guys Guide to Testing Network Vulnerability". Check out the following site.
http://www.misti.com/seminar_list.asp

Complimentary Publications

Two new documents are available for download from the ISACA web site: *Conducting Year 2000 Reviews During the Final Months Before the Millennium* and *COBIT Audit Guideline for Y2K Contingency Planning*. Both are ISACF publications.

What Are You Getting From Your Training Seminars?

By: Mitchell H. Levine

With audit departments under increased pressure to cut expenses, choosing the right training course is crucial. Throughout this article, various forms of training will be discussed and recommendations will be made for courses which are appropriate based on the experience level of an EDP auditor.

Training Courses Designed for EDP Auditors (Audit Training Inst.)

There are few training vendors who design their courses specifically for EDP auditors. The two types of courses offered consist of introductory and advanced courses for EDP auditors. Usually, they are not based on any specific technology.

The EDP audit courses that do not deal with any specific type of technology discuss controls at a generic level that should be in place based on the type of review that is performed (e.g., Data Center, Software Development Life Cycle, Application). These courses are designed to build the control perspective of an auditor and are more appropriate for a junior auditor. An auditor that is experienced in a specific technology area does not gain anything from these courses. This is because from a control perspective, the experience derived from one technology review can be applied to another technology.

The EDP audit courses that deal with a specific technology is used by an auditor to obtain the necessary knowledge to perform an audit of a specific area immediately after the training course. Some auditors may feel that they should receive a cookbook audit program from the training course which could then be applied to their specific environment. This is an unreasonable expectation since there are many site-specific factors which determine the control approach and technology solutions that are required to be used. The most important objective is to gain the necessary knowledge to build the customized audit program for any specific environment.

In order to gain the necessary knowledge from a technology training course, it is important to ensure that the scope of the course covers a typical data center environment. Specifically, a review of an operating system should include the controls provided by the external security systems. Fortunately, some operating system platforms, such as VAX/VMS, contain sufficient security built into the operating system. Therefore, the training course should only discuss the controls that are provided by the VAX/VMS security. However, operating systems like IBM's MVS, VM, and DOS have third party vendor external security products (e.g., ACF2) which are used by many installations. These products must be included within the scope of the training course.

Many training vendors may feel that a person should enroll in training courses that are specific for the external security product (e.g., ACF2, RACF, Top Secret) in order to obtain the information not provided in the operating system course. However, the scope of each these types of courses often neglect many of the critical control areas. For instance, a CICS course may discuss the internal security provided by CICS, but do they cover the external security interfaces for ACF2, RACF, or Top Secret? The same issue arises when one goes to a technology course for the security product. Do they discuss the security that is provided for CICS?

The reason that these critical controls slip through the cracks of training courses is in part due to the instructors lack of knowledge of all of these products. Does your MVS instructor have knowledge of ACF2, RACF, and Top Secret? Does your security product instructor have knowledge of CICS, MVS, Tape Management Systems (i.e., CA-1, TLMS), and Job Scheduling Systems (i.e., CA-7, CA-Scheduler)? Splitting the technology and the security into two separate courses does not ensure a better comprehension of both areas. The goal should be to know how they interact together.

There are limits to the length of training courses that must be considered when developing the scope of a training course. However, you should not be misled to think that when you attend a technology course you are covering all of the components of an audit.

Training Courses Provided by Vendors of Products

A critical issue that must be considered when selecting a training vendor is the overall technical background of the instructor. When using training vendors who designs their courses specifically for EDP auditors, the instructors themselves may not be privy to the detailed information provided by the vendor of the product. The alternative is to attend a training course that is presented by the vendor. Receiving training from the vendor who actually develops the product enables one to obtain all of the available technology information related thereto. However, the instructor of an Audit Training Institute may be able to present the topic tailored more to an auditor's perspective.

Training Courses Deigned to Explain Technology

Selecting the right training course for an advanced auditor who has overall knowledge about control requirements and technology is very difficult. Attending an Audit Training Institute or the courses offered by a vendor of a specific product may not provide any additional knowledge. A possible alternative is to attend a course which is designed for system programmers. This would enable the advanced auditor to gain a better foundation of the technology which would in turn open up new potential control areas. In addition, it would put the auditor on a more equal footing with the system



programmer when issues are discussed during the audit.

When attending a technology course that is not designed for auditors, the auditor must be able to intellectually build a bridge between the technology and the control requirements. It should be noted that when attending these courses, much of technology may not be understood by the auditor.



Another possible solution for advanced auditors is to use the allocated training budget to perform research on their own to increase their audit scope. However, unless there is a system programmer or the vendor of the product readily available to confirm the results of their research, an auditor can easily misinterpret the information that is obtained from the technical manuals.

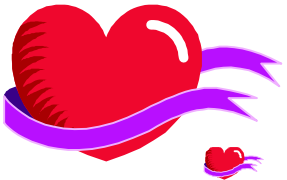
Exhibitions Which Include Training Sessions

Exhibitions which are used to allow vendors to promote their products, attempt to attract users by offering training courses. An auditor should investigate these courses thoroughly before taking the time to attend. This is because most of the instructors are the exhibitors themselves who spend more time talking about their products than the topic of the seminar.



Audit Conferences

Audit conferences present a unique opportunity to interact with many of one's peers and provide many training courses to choose from. The training courses are short sessions which can last from 2 hours to one full day. Many of these courses are offered by instructors who teach training courses for various training vendors and who offer an abridged version of the course for the conference. Since most of these courses are about general topics (e.g., MVS for auditors and ACF2), it is impossible to cover all of the control issues that would normally be discussed during a full training course. An auditor should not expect to attend these courses and be able to immediately start performing an audit based on the information provided. Rather, they would be better served if they attend the actual full length training course offered by the vendor. These audit conferences are appropriate for managers who are not responsible for performing the actual audits, but are required to have the knowledge of the high level control issues.



Vendor Conferences

Vendor conferences, such as the Security and Audit Conference offered by Computer Associates (CA), provide concurrent training courses which deal with specific topics. As demonstrated by Audit conferences where there is one course for a specific technology, CA offers approximately one dozen courses for each technology area. For example, some courses offered by Computer Associates at their last conference for specific topics within Top Secret includes:

- Top Secret SDSF interface
- Top Secret VTAM interface
- Top Secret CICS Enhancements
- Top Secret Security Database
- Distributing Top Secret Security
- Enhancing Top Secret Audit Trails
- Top Secret with IDMS



The instructors for the CA conference in many cases are the developers of the product who have the most knowledge of their products. The Computer Associates Security and Audit Conference is the highest rated training session on my recommended list for all auditors who are responsible for auditing MVS, DOS/VSE, VM, DB2, or VAX/VMS while using ACF2 or Top Secret security.

Conclusion

Choosing the right training course is a difficult task because there is for the most part, some aspect not covered. The best approach is to determine one's objectives and investigate each available course thoroughly beforehand.

Unless one has an audit and system programming background which enables you to interrelate all of the technology and control issues, training will be the main focal point for one's future development. Therefore, one should make the best use of training course selections.



Mitchell Levine is the President of his own consulting company, Audit Serve, Inc which is located in New Canaan, CT. He can be reached at levinem@auditserve.com



HAPPY VALENTINES DAY!!!

**Directions to Buckeye Hall of Fame Café
1421 Olentangy River Rd.
Columbus, Ohio (614) 291-2233**

From the North:

Take 315 S. to Kinnear Rd. exit. Go left around Lenox Square. Stay in the right lane. The Cafe is one block away on the right hand side.

From Downtown:

Take High St. or Neil Ave. (north) to 5th Ave. West (left). Turn right at Olentangy River Rd., after the bridge and the Cafe is on your left.

From the East:

Take 670 W. to Neil Ave. and travel north to 5th Ave. Turn left at 5th Ave. Once over the bridge, turn right onto Olentangy River Rd. The Café is on your left.

From the South:

Take I-71 N. to 670 W. Exit at Neil Ave. and go north to 5th Ave. Turn left at 5th Ave. Once over the bridge, turn right onto Olentangy River Rd. The Café is on your left.

Membership Information: www.isaca.org/memb1.htm