

OFFICERS AND DIRECTORS 2001-2002

PRESIDENT

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

VICE PRESIDENT

Carrie Schrader, CISA
Handleman Company
(248) 362-4400, Ext. 358

TREASURER

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

SECRETARY

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

DIRECTORS

Ed Barszcz, CIA, CFE
Facilities Chairperson
Blue Cross/Blue Shield of MI
(313) 225-9076

Karen Cordes, CIA, CISA
Consumers Energy
(517) 788-0439

Patti Earl-Cole, CISA, CIA
Student Relations Chairperson
Blue Cross/Blue Shield of MI
(313) 225-8577

William G. Garvey, CISA
Delphi Automotive
(248) 267-5723

Brenda L. Karl, CISA
Job Bank Chairperson
Jefferson Wells International
(248) 350-3006

Ray Kaslik, CISA, CIA, CFE, CMA
Seminar Chairperson
AAA Michigan
(810) 727-1962

Don Ledwith, CISA, CCP, CQA
Membership Chairperson
General Motors Corporation
(810) 492-1092

Michael Mullens, CISA, CIA
Cyndi Shelton, CISA
General Motors Corporation
(313) 665-0000, Ext. 44056

Mike Stolarczyk, CISA
Jefferson Wells International
(248) 350-3006 ext. 1319

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

Michael Tomasek, CISA, CIA
(810) 805-8191
Sander Wechsler, CPA, CISA
Ernst & Young, LLP
(313) 628-8024

Brent W. Wylie, CIA, CISA, CFE
Internet / Newsletter Chairperson
Blue Cross/Blue Shield of MI
(313) 225-0527

PAST PRESIDENTS

Todd McGowan, CPA, CISA
Deloitte & Touche, LLP
(313) 396-3407

Marci Klain, CPA, CISA, CIA
General Motors Corporation
313-665-0000, Ext. 44072



*Information Systems
Audit and Control
Association*

DATABYTE

NEWSLETTER OF THE DETROIT AREA CHAPTER

VOLUME 16, #5

REGION 2, CHAPTER 8

JANUARY, 2001

Monthly Meeting -- Joint meeting with CFE
Thursday, January 10, 2002

After Dinner Topic: "Making the Computer Crime Case:
The Challenge and How to Meet It."
Speaker: Terrence Berg

Location: Marinelli's restaurant
4924 Rochester Rd. Troy
Just North of 18 mile/Long Lake Rd.
There is no map available.
248/689/6460.

Date: Thursday, January 10, 2002

Time: 5:30-6:15 Registration/Networking
6:15-7:15 Dinner
7:15-8:15 After-Dinner Presentation

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

Reservations---Make your reservation by 4:00 PM, Monday, January 7. You can do online reservation at isaca-det.org. If you do not have access to the Internet, e-mail your reservation to Art Abruzzo at aabruzzo@amerisure.com or call him at (248) 426-7944. Please include your name, company, telephone number, and whether you are a member.

Visit our web site at: isaca-det.org

Message from your President...

Dear Members,

Welcome back! I hope everyone had a wonderful holiday and will have a happy, healthy and prosperous 2002. Once again our December meeting with the IIA was a great success. The two groups combined had over 140 people attending the meeting. I believe that is the largest joint meeting we have ever had. I think we should all be applauded for taking the time to advance our profession even at this most hectic time of the year. The presentations by Salman Aziz speaking on Firewalls and Scott Vowels talking about Penetration Testing were worthy of our large attendance. Our relationship with the IIA continues to be very strong and I look forward to future joint meetings with them.

Our January meeting will also be a joint meeting, this time with the Certified Fraud Examiners. Our topic of Cyber crime should once again be very timely and informative. I would hope we would all want to find out more on this topic. Please note the meeting will be on Thursday January 10, 2002 at Marinelli's Restaurant in Troy at 4924 Rochester Rd. Please check our website at isaca-det.org for more information. We will be back at Big Fish Seafood Bistro and will resume our usual Wednesday night meetings starting with our February 2002 meeting.

As we head into 2002, I believe our organization is as healthy as it has ever been. Our meeting attendance remains at a high level, our seminar attendance is exceptional, and we are reaching out to students at some of the local colleges and letting them experience what our organization is all about. However, to stay at this level we need your help, we are currently reaching that point in the year where we need to start thinking about recruiting new Board members for 2002 – 2003. There are a variety of ways you can serve the Chapter, please think about making a contribution to our chapter either through a Board position or serving on one of our committees.

As I mentioned earlier, the Seminar committees of both ISACA and the IIA have been working very hard over the past few months to put together another outstanding Spring Conference. The time period for this conference will be March 25 – 27, 2002 at the Lyon Meadows Conference Center. You should have already received information on this event or will be receiving it shortly. The course offerings are once again very timely and educational and at the price we are charging, they are the best bargain around. In this time of tightening budgets, we believe it is the best training value you will find and hope that everyone will take advantage of this opportunity.

I would once again like to stress to you, our members, that we (the Board) are here to serve the membership. If you do not believe we are adequately doing that or have a suggestion you think will help us do it better, please feel to contact me or any other Board member. You can reach me through e-mail me at aabruzzo@amerisure.com or call me at (248) 426-7944. You can also contact us through the website at www.isaca-det.org.

I look forward to seeing all of you at the January dinner meeting.

Art Abruzzo

Chapter President

MARK YOUR CALENDARS!

The Detroit Area IIA and ISACA chapters are again holding their annual Spring Conference at the Lyon Meadows Conference Center in South Lyon. The dates are March 25-27, 2002. The tracks, sessions and presenters are outlined below. Pricing, course descriptions, and other details are currently being finalized and a formal brochure will be distributed in late December. We will begin taking registrations at that time. Information will also be available at the ISACA website (isaca-det.org). Please direct any questions to Ray Kaslik at 586-727-1962 (email Kaslik@klondyke.net).

SPRING CONFERENCE OUTLINE

TRACK	SESSION DESCRIPTION	DATES	PRESENTER
Electronic Commerce	Control & Security of E Commerce	3/25/02	Gordon Smith (CANAUDIT)
	Hardening the Network for E Commerce	3/26/02	Gordon Smith (CANAUDIT)
	Understanding & Preventing E Fraud	3/27/02	Gordon Smith (CANAUDIT)
Internet & Network Security	Control & Sec. Of Wireless Networks	3/25/02	Paul Castillo (CANAUDIT)
	Penetration Testing	3/26/02	Paul Castillo (CANAUDIT)
	Control & Security of the Internet	3/27/02	Paul Castillo (CANAUDIT)
Risk Assessment	Digital Analysis Using Benford's Law	3/25-26/2002	Mark Nigrini
	Assessing Enterprise Risk for Audit Planning	3/27/02	Arthur Andersen
Computer Assisted Audit Techniques	ACL	03/25-27/2002	Ernst & Young
Introduction to Auditing	Introduction to IT Auditing	3/25-26/2002	Jeff Whitman (CANAUDIT)
	Writing Skills	3/27/02	Jefferson Wells
Value Added Audits	Contract Auditing	3/25/02	Jefferson Wells
	Consulting Excellence	3/26/02	Jefferson Wells
	Mergers & Acquisitions	3/27/02	Deloitte & Touche

Network Tools and Continuous Monitoring: Improving Audit Efficiency and Effectiveness

By: Eric Flegel, First Vice President and Audit Manager, ABN AMRO North America, Inc.

As you look at your department's annual audit plan, substantial portions of the high-risk areas were probably not even on the radar a decade ago. For example, most companies had never heard of firewalls, e-commerce was known as EDI with only a limited number of big players participating, and privacy legislation such as Gramm-Leach-Bliley and HIPPA had yet to be conceived. Information echnology audit professionals are consistently challenged to address these new audit risk areas with little or no increase in staffing. Implementation of a continuous monitoring program using automated network tools can be an effective way to improve both the efficiency and effectiveness of your information technology audit program.

When should a continuous monitoring program be considered?

Most audit areas can be potential candidates for a continuous monitoring program. Key factors to consider are:

- Relative risk associated with the activity to be monitored - In general, monitoring should be considered only for medium and high-risk activities.
- Source, availability and time required to gather and analyze the data – To be efficient and effective, the information needs to be reliable and readily accessible.
- Nature of the information – Monitoring programs typically are more effective when the information is quantifiable. Audit areas that are qualitative in nature are generally not as easy to monitor.

acceptable thresholds for these criteria and determine the frequency of your monitoring activities.

What are the benefits of a continuous monitoring program?

The information technology auditor can achieve several benefits from a continuous monitoring program:

- Increased audit value – Once developed, a continuous monitoring program can typically be executed in less time than a traditional audit, allowing more time to be focused on high-value activities.
- Increased audit coverage - Many audit departments provide advance notice of audit schedules. Have you ever wondered how much cleanup effort was done in the weeks or days immediately preceding the audit? A properly designed continuous monitoring program can provide a greater level of assurance to ensure that controls remain effective throughout the audit period.



HANDLEMAN COMPANY

Handleman Company, the leading supplier and merchandiser of music products for North America's leading retail chains and music labels is seeking a Senior Information Technology Auditor. The position entails independently conducting or supervising significant, broad scope and complex audits of information technology systems and procedures to assess the effectiveness of controls, accuracy of records, and efficiency of operations.

ESSENTIAL DUTIES AND RESPONSIBILITIES include the following. Other duties may be assigned.

- Examining systems and interviewing workers to ensure compliance with applicable laws and regulations.
- Participating in field audits of various business units, including analyzing policies and procedures relating to information systems, information security, operations functions, internal controls, and business processes.
- Conducting and documenting technical audits of mainframe, midrange, LAN/WAN and telecommunications systems.
- Participating on project initiatives and performing system development life cycle (SDLC)/conversion reviews to evaluate systems enhancements and development efforts.
- Analyzing data obtained for evidence of deficiencies in controls, duplication of effort, extravagance, fraud, or lack of compliance with laws, government regulations and management policies or procedures.
- Supervising, reviewing, approving the work of auditors, and preparing reports of findings and recommendations for management.
- Conducting special studies for management, such as those required to discover mechanics of detected fraud and to develop controls for fraud prevention.
- As necessary, participating on financial/operational related audit assignments.

QUALIFICATIONS:

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily in a highly visible environment. The requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

- Bachelor's degree in Information Technology, Accounting and/or Finance
- 3 - 5 years of proven public or internal informational systems auditing
- CPA, CISA or CIA is preferred
- Hardware/Operating system experience preferred: IBM mainframe/OS390, AS400, Unix, Sun Solaris, Windows NT and 2000, Novell, network infrastructure and desktop
- Software/Database experience preferred: Oracle database and ERP, Checkpoint firewall, ACL, ACF2, Bindview, supply chain software, EDI and MSAccess
- Financial/operational background is a plus in order to assess the impact of system implementations and changes
- Must be able to quickly assess risk within diverse company operations, establish audit review plans to efficiently and effectively evaluate the adequacy of related controls with minimal supervision
- Strong verbal and written communications and interpersonal skills are required
- Self-motivated with the ability to motivate others
- 25% Travel possible

Handleman Company offers a comprehensive benefits plan, including medical, dental, 401(K), pension, and merchandise discount on music product. We invite you to apply by sending your resume along with salary expectations to:

HANDLEMAN COMPANY

Human Resources/SIA • 500 Kirts Blvd. • Troy, MI 48084 • Fax: (248) 362-3656 • EOE

Continued from page 3

- Timely identification of problems or concerns – Have you ever found that controls in a business or technical area deteriorated significantly from the last scheduled audit? With a continuous monitoring program, you can identify and correct problems as they begin to develop. It is usually less time consuming to implement corrective action when problems are identified early.
- Ability to monitor trends – A continuous monitoring program can also be a useful tool for monitoring progress made in correcting open audit issues. For example, regular network scans can be used to monitor the information technology department's progress in removing FAT drives from a Windows NT network.
- Improved relationships – A continuous monitoring program can be useful in strengthening relationships with business unit (i.e. auditee) management. Through the use of continuous monitoring, the auditor is often perceived as business partner and not as a policeman. How should the results of a continuous monitoring program be reported?

How should the results of a continuous monitoring program be reported?

If you believe that audit's ultimate deliverable is improvement in the overall control structure of the organization, a strong case can be made for the following approach:

- Communicating exceptions to line management as they are found;
- Providing line management thirty days to implement corrective action; and
- In those cases where corrective action is not implemented within the thirty-day period, issuing a formal memorandum to communicate the exception. Similar to an audit report, copies of the memorandum should be provided to senior management. Line management should also be required to provide a written corrective action plan within 30 days with exceptions being tracked as open audit issues.

This approach provides a strong incentive to line management for timely implementation of corrective action.

Continued on page 5

After Dinner Presentation

"Making the Computer Crime Case: The Challenge and How to Meet It."

This presentation will discuss the scope of the problem of computer crime and will review strategies for responding to this problem. Michigan's laws defining computer crime will be examined and methods for successful investigations and security measures will be discussed.

Terrence Berg is an Assistant Attorney General and Chief of the High Tech Crime Unit for the Michigan Department of Attorney General. In May of 1999, he was appointed by Michigan Attorney General Jennifer Granholm to organize the Department of Attorney General's Internet and computer crime prosecution unit. Prior to joining the Michigan Department of Attorney General, Berg was an Assistant United States Attorney for the Eastern District of Michigan, from 1989 to 1999. Since starting the unit, Mr. Berg was awarded a fellowship which allowed him to work with the United States Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), in Washington, D.C., as part of a Computer Crime Fellowship sponsored by the National Association of Attorneys General ("NAAG"), for ten months. Mr. Berg has handled matters involving computer intrusion or "hacking," Internet auction fraud, child exploitation, Internet stalking, theft of trade secrets, Internet bomb threats, and other legislative, policy, and investigative matters pertaining to computer crime enforcement. He has lectured on legal aspects of computer crime at the American Bar Association's 2000 Annual Meeting in New York City, at the FBI Academy in Quantico, Virginia, and the National Advocacy Center in Columbia, South Carolina. His article, "www.wildwest.gov: The Impact of the Internet on State Power to Enforce the Law," appears in the December, 2000 issue of the Brigham Young University Law Review.

Continued from page 4

How to use network tools in a continuous monitoring program?

Today, many information technology departments employ various network-monitoring tools that can be leveraged by the information technology auditor to implement a continuous monitoring program. Listed below are samples of tools you may have available and how you might use them in a continuous monitoring program:

- Help desk software, such as Tivoli, can be used to monitor the number of help desk calls received on a monthly basis, the number of repeat calls (problem not fixed correctly on the first call), and the average time to close a trouble ticket. Depending on the nature of your organization, it may be useful to track this information by location and/or application. Unusual spikes or upward trends in help desk calls can be early warning indicators of system-related problems.
- Network monitoring software such as CA Unicenter can provide real-time monitoring of changes to the global parameters on networks. For example, CA Unicenter event codes can be used to identify changes in the domain policy for Windows NT domains. CA Unicenter can be configured to e-mail the auditor whenever there is a change in the domain policy. Changes to the domain policy should be infrequent and be approved by management.
- SMS can be used to monitor Windows NT networks for:
 - Servers or workstations that are not using the NTFS file system - Windows NT cannot provide file-level security if the drive does not utilize the NTFS file system.
 - Servers and workstations containing rollback.exe - Both Windows NT workstation and server are shipped with the rollback.exe utility. If run on a production system, rollback.exe removes all system registry entries without warning. Therefore, if a user runs rollback.exe, there is no system to rescue or to restore as the registry and the setup.log file no longer exist.
- Servers and workstations running without installed service packs - To ensure a secure and stable environment, all machines should be running current service packs.
- Tools such as Bindview and Enterprise Security Manager can be used to monitor Windows NT networks for:
 - Number of accounts whose last login date is more than 30 days from the current date - A large number of such accounts could indicate that deletion of accounts is not occurring on a timely basis.
 - List of accounts with a password age exceeding the password change policy - Assuming a password policy requiring passwords to be changed every 30 days, a report identifying numerous accounts with password ages exceeding 30 days could indicate problems enforcing compliance with policy.
 - Listing of administrator equivalent accounts - While administrator equivalent accounts are required, they are very powerful and their numbers should be held to a minimum. Periodic reporting of administrator equivalent accounts and comparison to established baselines can be a useful way to monitor control over these powerful accounts.
 - Listing of users with passwords set to never expire - User accounts should not be allowed to have passwords set to never expire.
 - Listing of global domain values - Parameter settings such as minimum password age, minimum password length, password uniqueness, and lockout parameters can be listed for comparison with authorized policies.
 - Password cracking tools such as L0phtCrack can be used to assess the relative strength of user password composition. These tools can provide dictionary, hybrid and brute force cracking analysis, and can be very useful in assessing the effectiveness of security awareness programs.

What if your information technology department doesn't have all these tools? You can still implement a continuous monitoring program. Much of the information reported by the tools listed above can be extracted through the use of scripts. It may take longer to perform the initial development when using scripts, but the process can be just as effective.

How do I get started?

The examples listed above focused primarily on the Windows NT platform. However, continuous monitoring programs can be implemented for any platform. Interview your systems personnel, find out what tools they use, be creative and see how you may use these tools in the audit process. In many cases systems personnel may already be running the reports that you require for your monitoring activities. If not, they may be able to develop them for you or provide you with access to generate your own reports. You will also need to make decisions regarding the specific criteria to monitor, establish

The Year At A Glance

Meeting Date	Pre-Dinner Topic	After-Dinner Topic
January 10, 2002 (Thu)	Joint meeting with ACFE	Cybercrime
February 20, 2002 (Wed)	Government Impact on Disaster Recovery	Network Contingency Plans
March 20, 2002 (Wed)	CISA Roundtable	E signature
April 17, 2002 (Wed)	Wireless Security	Internet Virus
May 15, 2002 (Wed)	CRM	Single Signon

Menu - January 10, 2002

Dinner will be served family style. No entree selection will be required except for a Vegetarian Plate.

The following entrees will be served:

CHICKEN PICATTA

BEEF BURGANDY

WHITEFISH

ITALIAN SAUSAGE & PEPPERS

DESERT: ICE-CREAM

DINNER INCLUDES: SOUP, SALAD, ROLLS,
VEGETABLE AND PASTA. POP, COFFEE AND TEA
CASH BAR WILL BE 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 in a cancellation. Your cooperation is greatly appreciated.

DATA BYTE

Information Systems
Audit and Control
Association
DETROIT AREA CHAPTER
P.O. BOX 4297
TROY, MICHIGAN 48099-4297

