

Control Bits & Audit Bytes

Western Michigan *INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION* Newsletter

FEBRUARY 2001 NEWSLETTER

OFFICERS

PRESIDENT

Rick Cummings, CISA
Jackson National Life Insurance Co.
One Corporate Way
Mailstop 538
Lansing, MI 48958
517 / 367-4301
FAX: 517 / 394-1795
rick.cummings@jnli.com

VICE PRESIDENT

James Green, CISA
Arthur Andersen
Technology Risk Consulting
Suite 700
171 Monroe Avenue NW
Grand Rapids, Michigan 49503
(616) 653-8364
FAX: (616) 653-6305
james.a.green@us.arthurandersen.com

SECRETARY

John Blair, CISA
Steelcase, Inc. CH-3E-18
P.O. Box 1967
Grand Rapids, MI 49501-1967
616 / 246-4730
FAX: 616 / 248-7550
jblair2@steelcase.com

TREASURER

Pam Bradford, CISA
National City, K-A16-C7
One National City Pkwy
Kalamazoo, MI 49009-8002
616 / 376-7523
FAX: 616 / 376-4408
Pam.bradford@national-city.com

BOARD OF DIRECTORS

CISA COORDINATOR

Michael Sekoni, CISA
Accident Fund of Michigan
P.O. Box 40790
Lansing, MI 48901-7998
517 / 342-4200 ext. 721
FAX: 517 / 342-4299
michaels@accidentfund.com

NEWSLETTER EDITOR

Rick Cummings, CISA
Jackson National Life Insurance Co.
5901 Executive Drive S52
Lansing, MI 48911-5389
517 / 367-4301
FAX: 517 / 394-1795
rick.cummings@jnli.com

PAST PRESIDENT

John Arens, CPA
Meijer, Inc. MC 985/4
2929 Walker Avenue NW
Grand Rapids, MI 49544-9428
616 / 791-3521
FAX: 616 / 791-5341
arensj@meijer.com

DIRECTOR AT LARGE

Kim Coyer
Independent Bank Corporation
623 Washington Ave
Bay City, MI 48708
(517) 892-3511
kcoyer@ibcp.com

March Dinner Meeting

March 14, 2001

Sheraton Lansing @ I496 and Creyts Rd.

Auditing IT Governance

By Sander S. Wechsler, CPA, CISA

Auditing IT Governance, a paradigm shift in auditing IT or nothing more than a new name for current IT audit practices? In this timely presentation, attendee's will be provided with an overview of auditing IT Governance and why these audits are increasing in regularity. Attendee's will also be provided with information on the objectives of these audits and the scope of work that would be covered in an audit of IT Governance. Finally, attendee's also will be provided with an overview of the kinds of procedures that would be performed in a typical audit of IT Governance.

Speaker BIO

Sander S. Wechsler, CPA, CISA, is a Senior Manager in the Information Systems Assurance and Advisory Services Practice of Ernst & Young, LLP. He has over 10 years of technology based audit experience. He has significant knowledge and experience in the audit, control and security of enterprise resource planning application software. Additionally, Mr. Wechsler has performed multiple reviews of various eCommerce implementations as well as provided consulting services on the strategic, operational and control issues associated with these systems.

He is currently a member of the American Institute of Certified Public Accountant's SysTrust Task Force and a past member of the Continuous SysTrust Task Force. Sander is also a member of the Information Systems Audit and Control Association's Standards Board.

Please make your reservation and meal selection (see below) by March 8th!

Call John Blair and make your reservation today!! **(616) 246-4730**

OR e-mail John at jblair2@steelcase.com

Costs - \$25 Non Members / \$22 Members

Dinner menu:

- 1- Pork
- 2- Turkey
- + Salad
- + Dessert

4:00 5:00 Board Meeting
5:00 5:30 Social Hour / Registration
5:30 6:30 Presentation
6:30 7:30 Dinner

Presidents Message

We are beginning to seek nominations for Chapter Board Position for the 2001/2002 season. Everyone is encouraged to submit nominations (including yourself) for any one of the Officer positions on the Board. All positions are for a one-year tenure. The Officer positions are elected positions, and the Directors are volunteers, which are appointed by the board. Positions that we are looking for nominations are President, Vice President, Treasurer and Secretary. Volunteers are also needed for the Board appointed positions of 'Director at Large' and 'CISA Coordinator'. Here is a chance to have a direct influence on how your board serves its membership!! We will be providing a list of duties for each position in the next newsletter or separate mailing. If you are interested in helping the chapter (and receiving extra CEU for certification), please send your nominations to the Official Election Officer, Mike Grinwis at Michael.Grinwis@jnli.com. Please support your local chapter by nominating a fellow member or volunteering your own services. This is a great way to network, provide input into the chapter events, and adds to your business resume.

Spring Seminar –April 19 and 20

Topic: Privacy - Audit Strategies
Date: Thursday and Friday April 19 and 20
Facility: National City - Kalamazoo
Lunch provided.

Speaker: Michael (Mick) Neshem

Pricing: \$250 ISACA Members or if 3 or more from same business attend
\$275 Other Association (IIA, AITP, AICPA, etc.)
\$300 Non-Members

Registration: Limited to 40 people.
Steelcase Inc.
c/o John Blair
m/c CH-3E-18
PO Box 1967
Grand Rapids, MI 49501-1967
(616) 246-4730, but payment will confirm your registration.

Privacy concerns for personal information and legislative actions have increased the awareness and ramification of security risks. Please join us April 19 and April 20 as Michael (Mick) Neshem leads us through a seminar discussing the risks, controls and action items within the corporate infrastructure.

This seminar will provide the auditor and IT professional with knowledge to classify data, assess the importance of securing information, developing a balance between privacy and cost to secure and an understanding of infrastructure control points.

Detail Seminar Synopsis and Speaker Bio will be published in the next few days

Rick Cummings

Western Michigan Chapter IIA

Spring Seminar

The Western Michigan Chapter IIA will be hosting a 1-day seminar on fraud, conducted by Courtenay Thompson. Courtenay is a well-respected expert on fraud and will be conducting one of his brand new seminars – Fraud 2001. Please see below for details, including a seminar outline and Courtenay's bio.

The seminar will be held in Grand Rapids at Duba's restaurant on Thursday, April 5. Duba's is located at 420 E. Beltline NE (near the I-96 crossing). The cost to attend is \$140, which includes continental breakfast, lunch, and various other snacks and beverages throughout the day.

Tentative Schedule for Thursday, April 5:

8:00am to 8:30am	Breakfast and Registration
8:30am to 12:00pm	Presentation (break midway)
12:00pm to 1:00pm	Lunch
1:00pm to 4:30pm	Presentation (break midway)

To register, please contact Peter Dann by noon on Friday, March 16.

Phone: (616)475-2320

Email: pdann@steelcase.com

FRAUD 2001

This course explores current fraud-related challenges facing auditors and their organizations and provides practical proven solutions to real problems. The program is highly participative. Attendees will have the opportunity to share their questions and greatest fraud-related concerns, and share their own proven techniques and ideas.

- Fraud - What All Auditors Must Know!
- Getting Executive Commitment
- Fraud Implications of a Changing Business Environment
- Lessons From Recent Major Cases
- What is New in Fraud!
- Fraud-related Best Practices
- Mistakes to be Avoided
- Practical Approaches to Fraud-related Controls
- More Effective Detection

COURTENAY M. THOMPSON JR.

Mr. Thompson is a recognized authority on training managers, auditors and investigators in fraud-related matters. Since 1981 he has designed and presented courses on fraud prevention, detection and investigation for business and government organizations worldwide. Mr. Thompson is currently editor of "Fraud Findings" in The Internal Auditor magazine. Mr. Thompson's experience prior to entering the consulting field includes public accounting with a Big 5 CPA firm, audit supervisor for consumer financial services for a large retailer, and director of auditing for a life insurance company. His career in public accounting and internal auditing provided exposure to a number of types of impropriety including embezzlement, insurance fraud, loan fraud, stock fraud, kickbacks and bribery, misappropriation of funds and mail fraud. Courtenay Thompson received his BBA and MBA degrees from Southern Methodist University and is a Certified Public Accountant.

Internal Audit "Helpers" Newsletter from Audit Services

Some more ideas to "help" you, the professional internal auditor! If you have any difficulties accessing the web pages directly from this email, the newsletter is also posted on our web site at: www.auditservices.com/helpers.html

Let us know if we can be of any help.

XX

AUDITING THE INTERNET, E - BUSINESS/COMMERCE

Evaluating the controls over SNMP (Simple Network Management Protocol)? Go to <http://www.auditservices.com/itsnmp.html> for some assistance in auditing SNMP.

YOU can audit the internet! We can provide you with the tools, assistance and appropriate knowledge base to allow you to conduct an **internet** audit.

XX

CRSA (Control Risk Self Assessment)

Do you have the technical and other skills required to be a successful facilitator when conducting self assessment workshops? Good facilitation skill sets are "key" for a successful CRSA workshop.

Refer to our checklist at <http://www.auditservices.com/crsaskills.html> for a quick personal assessment.

XX

SAMPLING

Statistical sampling is either going to be an "attributes" or a "variables" test. Do you know when to use a variables sampling test? For a quick "refresher", review some of the characteristics associated with a variables sampling plan at our web page, <http://www.auditservices.com/ssvar.html>

Also, go to <http://www.auditservices.com/ssindex.html> for an outline of our one day Sampling Seminar.

XX

AUDIT TESTS

Have you ever tried to determine the effectiveness of your audit tests? Based upon your professional judgement, you can predict the probability of the effectiveness of your audit tests.

Go to: <http://www.auditservices.com/atestsprob.html> for an illustration of how you may be able to use this technique.

XX

AUDIT FINDINGS

To ensure adequate and proper reporting of audit results, it is essential that potential audit issues be thoroughly developed.

Enhance the probability of reporting on only key issues by following the C - C - C - E approach. For further details, refer to <http://www.auditservices.com/afind.html>

XX

FRAUD AUDITING

When conducting fraud audits it is important to recognize what type of fraud was perpetrated
Refer to <http://www.auditservices.com/fraudtypes.html> for a brief discussion of the two types of fraud.

XX

TRAINING

Feel free to take advantage of our **special offer** while it lasts: a customized in-house seminar for \$800 plus related expenses. For available dates and other information about our training initiatives go to <http://www.auditservices.com/auction.html>

As seen in the media . . .

A very UN-scientific approach to gathering meaningful information from the “giga-tons” of electronic and printed material that intrudes into our lives . . . and is occasionally actually worthwhile! Here are some of the latest “discoveries” . . .



1984 + 17 . . .

★ ★ ★ ★

Security Wire Digest, Feb 5, 2001,

www.infosecuritymag.com

- On January 31st, the U.S. Commission on National Security urged the Bush administration to create the National Homeland Security Agency (NHSA), and include a National Crisis Action Center as a "focal point for monitoring emergencies and for coordinating federal support in a crisis to state and local governments, as well as to the private sector."

The bi-partisan commission, lead by former senators Gary Hart (D-Colo.) and Warren B. Rudman (R-N.H.), recommended the formation of the NHSA to oversee government and private sector efforts to protect the nation's critical infrastructure from both physical and cyberattacks.

The commission report "recommends a new National Homeland Security Agency to consolidate and refine the missions of the nearly two dozen disparate departments and agencies that have a role in U.S. homeland security today," said commission Executive Director Charles Boyd, a former U.S. Air Force general.

The commission's recommendations are intended as a blueprint for matching the known and anticipated threats to national security over the next 25 years. Newt Gingrich, a commission member and former speaker of the House of Representatives, said the mounting threats in cyberspace--either by hostile nation states, terrorists or malicious hackers--will be a greater threat to the United States than any conceivable conventional war.

"In addition to weapons of mass destruction, we have to worry about Internet-based weapons of mass disruption," said Gingrich, now an IT consultant, in an interview with *Security Wire Digest*.

The new agency would be charged with planning, coordinating and integrating various U.S. government security activities and would be responsible for coordinating government and private sector efforts to address the nation's vulnerability to attacks.

<http://www.nssg.gov/phaseIIIwoc.pdf>

(752KB, 148 pages)

(Ed. Note: From Congressman to IT Consultant in one election!?! Where's my career counselor?)

Oooooopsssss . . .

★ ★ ★

Security Wire Digest, February 5, 2001

www.infosecuritymag.com

- Following the recently publicized BIND vulnerabilities the security firm warned of, source code masquerading as an exploit was posted to the popular Bugtraq mailing list. It installed a Trojan horse in any computer on which the code was run and then used the zombies to flood Network Associates's Web site with tens of thousands of messages, blocking access to the site for 90 minutes.

Elias Levy, moderator of Bugtraq and CTO of SecurityFocus.com, said it's likely that some of the list's 35,000 subscribers ran the program and unwittingly participated in the attack on NAI's DNS server. But he said Bugtraq did not err in posting the message.

Another list moderator agrees. "It always has been buyer beware. If you are subscribed to a list, you are accepting that you may get stuff you don't like--it's not without warning," said Russ Cooper, editor of

NTBugtraq and surgeon general of TruSecure Corp. "I would say that the responsibility for this lies with the users on the list who ran the code without looking at it.

While there may be finger pointing, Bugtraq and those who unwittingly launched the DDoS are not likely to face legal ramifications because of the inadvertent nature of the incident.

And You Think YOU'VE Got Problems . . .

★ ★ ★

Security Wire Digest, February 5, 2001

www.infosecuritymag.com

- Computer systems at more than 60 District of Columbia government agencies are at risk because of poor computer security practices at the District's Department of Public Works (DPW), the General Accounting Office (GAO) reported January 30th. A GAO security audit found that the District's DPW had not adequately limited employees computer access. More than 4,300 users had access to 20 software libraries, which could be used to bypass network security controls. The report also noted that interconnections with other agencies didn't limit these security problems to the DPW alone. The agency makes use of the District's WAN, connecting to 60 other organizations including the Metropolitan Police Department, the District General Hospital and the public school system.

In addition to poor access controls, auditors found that IDSeS only have been installed on two of the WAN's 22 access points. <http://www.gao.gov/new.items/d01155.pdf>

AOL Gets a "Bug"

★ ★ ★

Security Wire Digest, February 5, 2001

www.infosecuritymag.com

- As if AOL/Time-Warner needed another thing to worry about besides their merger, a year-old Trojan dubbed APStrojan.qa has gone on an AOL e-mail rampage, doubling the number of infected computers in the past 30 days and earning a medium-risk rating from antivirus software vendor McAfee.com. McAfee reported the steep increase last week, though AOL officials denied the pervasiveness of the virus.

According to McAfee, the virus message comes with a title of "hey you", and includes an attached Visual Basic script labeled mine.zip. Opening mine.zip activates the password-stealing program, and if you have AOL 4.0 or 5.0, everyone on your "Buddy List" becomes the next recipient of this rather nasty bug. Version 6.0 of the AOL software does not allow the bug to replicate, but it still steals passwords. As of Feb 1, over 200,000 PC's had been infected.

U.S. Falling Behind"

★ ★ ★ ★

CNN News On-Line, February 12, 2001

www.cnn.com

- The U.S. is increasingly vulnerable to attack because the monitoring agency responsible for early detection is losing the technology war to well-heeled, techno-savvy rogue groups, the head of the NSA said in an interview released on Monday. NSA Director Gen. Mike Hayden is interviewed for a CBS "60 Minutes II" program to be aired Tuesday, February 13th, 2001. In it, he said the bombings of two U.S. embassies in Africa in 1998, for example, were orchestrated without detection because Saudi dissident Osama bin Laden's group, which the government alleges was behind the attacks, had better equipment. "Osama bin Laden has at his disposal the wealth of a \$3 trillion a year telecommunications industry that he can rely on," Hayden said in a broadcast to air on Tuesday. "We are behind the curve in keeping up with the global telecommunications revolution," he added.

The CBS report is being aired as four men linked to bin Laden stand trial for their alleged roles in the embassy bombings in Kenya and Tanzania that killed 224 people, including 12 Americans.

The "STAR" guide:	★ ★ ★ ★ = Too good not to pass on!	★ ★ = Good stuff — it helps
	★ ★ ★ = Better than expected!	★ = Worth noting

(NT-ALT-DEL)

Taking a hint from "Men in Black", it's somewhat surprising what truthful tidbits can be obtained from the "gossip columns" of the IT world (and other "questionable" sources). Here's some of the latest "fluff" . . .

- ☺ Can't get enough news **AND** animation??? *eWEEK* (formerly known as PCWeek), has now launched it's own on-line TV news delivery at <http://www.Zcast.tv>. Get your daily dose of IT news from those wonderful folks at Ziff-Davis publishing, including The Dodge Report, Rumor Central, *eWEEK* Labs, etc. P.S. . . . Shockwave software is a requirement to view Zcast.tv.
- ☺ Looking for a working demo of Lotus' nifty Sametime 2.0 audio/video conferencing software? So is Lotus. Lotusphere attendees were somewhat baffled by the lack of a working demo after last September's "public" beta release.
- ☺ The foreign parent of a U.S. company presents IT management with a draft revision to the corporate security manual. IT Management asks Internal Audit to review and advise. I.A.'s review finds a significant number of conflicts between systems, operations, and responsibilities, including more than a handful of potential violations of state and/or federal statutes. The "kicker" — foreign parent's external auditors had **already signed off** before delivering the draft revisions to the subsidiaries! I.A. recommended IT Management summarily reject all revisions, which IT did. (*Ed. Note: – Well, at least they ASKED!!!*)

-
- ☺ On a TOTALLY NON-IT/NON-SECURITY NOTE: Those of you who will be traveling in and around the Lansing, MI area this spring and summer should take heed about finding alternate travel routes. I-496, which runs between I-96 on the west side of town, and US-27 on the east, will be shut down as of April, 2001!

The project is being conducted in two phases. Phase I closes the east half of I-496, from Pine St. (downtown) east to US-27, until completion. Phase II closes the western half (from I-96 to Pine St.) **after** Phase I is completed. You can dig up more info on the construction at <http://www.fix496.com>.

Looking for a good source of on-line I.T. info? Check out <http://www.techrepublic.com/>.



*Information Systems
Audit and Control
Association*

Education

The "Ultimate Update" returns with three ways to enhance your skills and learn how to leverage the latest advances in Transaction and Messaging systems. With three enrollment options, there's enormous value for architects/ designers/ decision makers, application developers, and system programmers.

WHEN: June 4-8, 2001

WHERE: Salt Palace Convention Center; Salt Lake City, Utah

CICS TECHNICAL CONFERENCE - \$1,775

Plug into high-voltage sessions on the topic of the year - how CICS can electrify your e-business opportunities. Explore possibilities related to Java and Enterprise JavaBean support. See how CICS applications easily integrate with WebSphere. Grasp the latest on Java, XML, and more. There's huge value for Classic CICS users. Plus, get set for details on a dynamite product announcement! Find topics galore on design/ architecture/system analysis, application development, and system programming functions.

MQSERIES TECHNICAL CONFERENCE - \$1,775

Business process management is key! Attend this conference to unlock the exciting new ways MQSeries can help master business integration and business process challenges! Get updates on the family of Message Queue Managers. Learn how MQSeries Integrator manages messaging better than ever, and discover vital new ways MQSeries Workflow can streamline your business processes. Explore MQSeries and WebSphere, plus Java, new messaging APIs, XML, clustering, and more. Are you implementing/tuning systems, creating applications, or architecting/designing? Tons of MQSeries sessions can help!

TRANSACTION AND MESSAGING CONFERENCE - \$1,875

Your third enrollment option lets you attend sessions from both the CICS Technical Conference and the MQSeries Technical Conference.

Three enrollment options - one focused purpose - to help boost your knowledge of the advances that can ignite e-business and lift your transaction and messaging systems to new heights!

- * 4-1/2 information-packed days in Salt Lake City
- * Dozens of skill-building elective sessions
- * Expanded Product EXPO with demonstrations
- * Lively birds-of-a-feather discussions
- * Shared customer experiences that can help save time and hassles.

For more details, call 800-IBM-TEACH (426-8322) and reference priority code 100PG002 or visit our conference Web site at:

<http://isource.ibm.com/cgi-bin/goto?on=c2274conference>

Job Market

Hello- my name is David James, I am the president of David James Search. We are a search firm who for the past ten years has been dedicated to the advancement and placement of Internal Audit professionals. In the year 2001, there was a calculated decision made that the focus would be on and in the area of Information Technology and I.T. audit related search.

Unlike most recruiters, I have decided not to post an erroneous position that does not exist in an attempt to get you to send me a resume. However, what I do want is to invite you to initiate a relationship. If you need or want a better position, for any reason, please call me or email me at david@davidjamessearch.com .

Most respectfully,

David L James

909-719-1484

My name is Larry Larsen and my wife and I own **Skyline Search**, an executive recruiting firm. We specialize in internal audit and are currently trying to fill several positions:

Senior Staff Auditor Salary \$45,000-\$55,000

Major U.S. Airline needs a Senior Staff Auditor. Paid relocation to southern U.S. This is a great company with great benefits including **free personal air travel**. Bachelor's degree in business and accounting required along with at least three years accounting or internal audit experience. CPA, CIA, or CMA certification a big plus. About 30% travel, both domestic and international.

IT Audit Manager Rural Mass. Salary \$75,000 - \$90,000

IT Audit Manager in small Massachusetts town. NYSE Company needs CISA with 8+ year's experience. CIA designation and ACL experience would be a plus. Specific systems include IBM AS/400, Sun Solaris/Unix, Open VMS and Windows NT. Also Novell and NT Networks experience.

Staff or Senior IA Central PA Salary \$40,000-\$60,000

Financial and operational internal auditor for NYSE manufacturing company located in central Pennsylvania. Public accounting experience a plus. Exposure to a manufacturing environment a big plus. This company has excellent benefits and a great bonus program. This is a new position and could be either staff or senior level, depending on the candidate's experience and background. They would prefer a CPA that would like to eventually move from internal audit into accounting management. Salary depends on experience.

Staff or Senior IA Kansas City Salary \$45,000-\$55,000

Staff Internal Auditor with a financial services company. This position is located in Kansas City, MO. Two years experience plus either a CPA or CIA designation. Great opportunity for advancement.

Staff Auditor Salary \$40,000-\$45,000

Major U.S. Airline needs a Staff Auditor. Paid relocation to southern U.S. This is a great company with great benefits including **free personal air travel**. Bachelors degree in business and accounting required along with at least one year accounting or internal audit experience. CPA, CIA, or CMA certification a big plus. About 30% travel, both domestic and international.

If you are interested or know someone that might be, send me an email at skylinerearch@yahoo.com and we can arrange to chat on the phone. Thanks for your help.

Larry Larsen

Final Words

Don't Forget.....
March Dinner Meeting
AND
Nominations for Officers

March 14, 2001
Lansing Sheraton @ I496 & Crytes Rd.

Control Bits and Audit Bytes is a publication of the Western Michigan Chapter of the *Information Systems Audit and Control Association (ISACA)*. The purpose of this publication is to disseminate useful and timely information on automated systems control and security issues to Chapter members and selected practitioners of computer systems audit and security. Articles, submissions, and advertisements are the responsibility of the submitter, and do not reflect the opinions, beliefs, or practices of the Western Michigan Chapter.

Materials submitted for publication in *Control Bits and Audit Bytes* must be received by the Newsletter Editor no later than the submission deadline published in the newsletter. If no submission deadline is published, the default deadline is approximately three weeks prior to the next scheduled meeting of the Western Michigan Chapter of the *Information Systems Audit and Control Association*.



*Information Systems
Audit and Control
Association*