

**OFFICERS
AND
DIRECTORS
2003-2004**

PRESIDENT

John W. McCormick, CISA, CIA
City of Detroit
(313) 224-4039

VICE PRESIDENT

Karine F. Wegrzynowicz, CISA
Ford Motor Company
(313) 337-5796

TREASURER

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

SECRETARY

Patricia A. Earl-Cole, CISA, CIA
Blue Cross Blue Shield of MI
(248) 633-2424

DIRECTORS

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

Salman Aziz
Delphi Automotive
(248) 813-8034

Edward R. Barszcz, CIA, CFE
Blue Cross Blue Shield of MI
(313) 225-9076

Michael A. Forrest, CISA
Jefferson Wells International
(248) 350-3006

Paul L. Haley, CISA
DTE Energy
(313) 235-9244

John H. Hoppesch, CISA
Handleman Company
(248) 362-4400 ex. 6718

Robert J. Otten, CISA, CIA
Kmart Corporation
(248) 463-2428

Brandy A. Pfeiffer, CISA, CPA
Federal-Mogul Corporation
(248) 354-2602

John L. Quaine II, CISA, CPA, CIA
Blue Cross Blue Shield of MI
(313) 225-7663

Carrie E. Schrader, CISA, CBM
Deloitte & Touche LLP
(313) 396-2754

Michael S. Stolarczyk, CISA
Jefferson Wells International
(248) 226-1319

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

Douglas S. Wahr, CISA, CISSP
The Auto Club Group
(313) 436-7488

Robert V. Yanik, CISA
City of Detroit
(313) 224-3101



Information Systems
Audit and Control
Association

DATA BYTE

NEWSLETTER OF THE DETROIT AREA CHAPTER

VOLUME 18, #4

REGION 2, CHAPTER 8

DECEMBER, 2003

Monthly Meeting Tuesday, December 9, 2003

JOINT MEETING WITH THE DETROIT CHAPTER IIA

Pre-Dinner Topic: "HIPAA"
Fredrick C. Heller, III, CISA

After-Dinner Topic: "Audit Committee Perspective – What's Changed"
Eric Hespenheide, Partner, Deloitte & Touche LLP

**PLEASE NOTE MEETING DATE IS THE SECOND TUESDAY OF THE MONTH
INSTEAD OF THE THIRD WEDNESDAY AND MEETING LOCATION AND TIME OF
MEETING IS DIFFERENT**

Date: Tuesday, December 9, 2003

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

Location: Ford Motor Conference & Event Center
1151 Village Road
Dearborn, MI 48124-5033
(313) 323-1972
Map on Page 5 of this Newsletter

Cost: \$25.00 Members
\$35.00 Non-Members
\$10.00 Students and Retirees

Reservations will be taken by Suzanne McCormick. Please make reservations by 6:00 P.M. on Thursday, December 4, 2003. You can make your reservation online at isaca-det.org or e-mail your reservation to Suzanne McCormick at jsmccor65@aol.com. If you do not have access to the Internet, call Suzanne at (248) 471-3075. Please include your name, certification, company, telephone number, and whether you are a Member, Non-member, Student or Retiree. All e-mail reservations will receive a personal confirmation that the reservation was received. Walk-ins are welcome.

Visit our web site at: isaca-det.org

Letter from the President

Dear Members,

December is our annual joint meeting with the IIA and this year it will be at the Ford Conference Center in Dearborn. Be sure and check out the map on page 5 as to where the site is. Both of the topics for December are timely; both will target the IIA and ISACA members in attendance.

Fred Heller, Director of Technology for Jefferson Wells is speaking on HIPAA, a regulatory subject about which all auditors should be aware. HIPAA requires the industry to standardize around a single set of formats related to acquiring, claiming and reimbursing for health benefits and services. Virtually everyone who provides or pays for healthcare is affected by HIPAA, including patients, hospitals, physicians, retail pharmacies, insurers, laboratories, health plans, **employers**, and companies selling products and services to the healthcare industry. In the area of privacy, HIPAA has teeth, as criminal penalties can be imposed for non-compliance, under certain circumstances.

Eric Hespenheide, Global Managing Partner, Deloitte & Touche is speaking on "Global Internal Audit Practices". It is always better to understand the best practices of your industry and Eric promises to bring a global perspective that should benefit us all.

From the International:

The International is encouraging each of you to take advantage of the online payment of dues. I tried it on November 1, and it was easy to follow. If you are comfortable with using your credit card online, this is the way to go. Your president received statistics about the growth of ISACA at the international and at the local level. Did you know that the major growth is in Asia (242% since 1997) and the least growth is in Oceania (14% since 1997)? However, total member counts look a little different: North America is the biggest with 14802

members; and Latin America is the smallest with 1011 members. Asia has 7823 members. Patti Earl-Cole, Chair of the membership committee, is working to make sure that Detroit does its part to grow our chapter this year by contacting the top industries in the metropolitan area. If any of you want to volunteer to assist her in these efforts, give her a call or email.

Do not forget to register early for the CISA and CISM exams and take advantage of the break in prices. Registration deadlines for the 2004 exams are:

Early: 4 February 2004

Final: 31 March 2004

Back at your local chapter:

The joint IIA/ISACA Spring Seminar will take place March 22 through March 24, 2004 at the **Ford Conference Center**. Unfortunately, with our increased attendance, we have outgrown the facility at South Lyon. We want to express our most sincere appreciation to Blue Cross Blue Shield of Michigan for their unwavering support in past years to make the seminar the success that it has become. You will be seeing additional information on the seminar through various media. Please make plans and sign up early so that you can take advantage of this great opportunity to learn at an economical price.

Come and join us at the Ford Convention Center in December and network with our IIA peers in what promises to be a great evening.

John W. McCormick, CISA, CIA
President
Detroit Chapter ISACA

PRE-DINNER INFORMATION

“HIPAA”

Fredrick C. Heller, III, CISA

Fred is currently the Technology Director for the Philadelphia office of Jefferson Wells and has more than 20 years of experience providing both internal and external clients with processes and methodologies to assess and mitigate risks. His industry experience includes over 15 years in the Healthcare sector. Fred has directed and/or completed many projects for Healthcare clients, including HIPAA Assessments, Vulnerability Assessments, and Risk Identification/Mitigation projects. His strengths lie in his ability to understand and communicate risk issues for all levels of management and the ability to develop a team when working on large complex projects.

Fred has served as the Director of Internal Audit (DIA) for one of the largest healthcare providers in the United States. As the DIA, he was responsible for a risk mitigation project related to Year 2000, the implementation of a corporate compliance office, and the initiation of a HIPAA task force. Fred has completed presentations to the Association of Healthcare Internal Auditors, Financial Executives International, New Jersey Bankers Association and several other special interest groups. Topics covered during his presentations include Network Security and HIPAA, Business Continuity Planning and Process Improvement, and IT Audit and Control - the Forgotten Aspect of Sarbanes-Oxley. Fred has been a member of ISACA and a CISA for over twenty years.

Presentation Outline

Fred’s presentation will focus on the HIPAA security requirements and expectations and will also provide attendees with the current state of HIPAA preparedness based on client interactions and a roadmap to helping your company comply with HIPAA security requirements.

- HIPAA Updates
- Post April Observation/Activities
- Current State of Activities – Sanity Check
- HIPAA Security Requirements and Definitions
- Process for Compliance
- What next?

AFTER DINNER INFORMATION

“Audit Committee Perspective – What’s Changed?”

Eric Hespeneide, Partner, Deloitte & Touche LLP

Eric Hespeneide is the leader of the US firm’s Audit Services practice, which includes both internal and external audit services. He is also the global leader of the firm’s Internal Audit Services practice and serves on the firm’s Sarbanes-Oxley Internal Controls Steering Committee, helping to develop the firm’s response to the Act and its related regulations.

Eric Hespeneide will address the changing priorities of audit committees in light of recent regulations and the current focus on corporate governance. He will discuss new activities that audit committees have undertaken in the area of risk management and the audit committee’s role in assessing an organization’s control environment, as well as the evolving role of internal audit and how it has impacted the expected relationship between the chief audit executive and the audit committee.

**TIME IS RUNNING OUT!
APPLY FOR CISM UNDER THE
GRANDFATHERING PROVISION TODAY!**

CISM™ (Certified Information Security Manager™) is a groundbreaking credential specifically designed for information security managers. More than 1,000 information security professionals have become CISM’s, and are among the first to be recognized for their expertise in information security governance, risk management, program development and incident response.

Until 31 December 2003, those who have eight years or more experience in information security, with a minimum of five years of information security management experience, may qualify to earn the CISM without taking the exam. For more details and to download a CISM grandfathering application, please visit www.isaca.org/cism.

YEAR AT A GLANCE

December 4, 2003	Reservations due by 6:00 p.m. for the December 9 ISACA/IIA dinner meeting
December 9, 2003	Chapter Meeting (Please Note: This meeting is on the second Tuesday of the month instead of the third Wednesday) <i>Joint meeting with the IIA</i> “HIPAA” – Fred Heller, Director of Technology, Jefferson Wells International “Audit Committee Perspective – What’s Changed?” - Eric Hespeneide, Partner, Deloitte & Touche LLP
December 9, 2003	Deadline for the January issue of the Databyte
January 9, 2004	Reservations due by noon for the January 14 ISACA/CFE dinner meeting
January 13, 2004	Deadline for the February issue of the Databyte
January 14, 2004	Chapter Meeting (Please Note: This meeting is on the second Wednesday of the month instead of the third Wednesday) <i>Joint meeting with the CFE</i> “Forensic Auditing” – Roy Parry
February 4, 2004	Early Registration Deadline for June 2004 CISA and CISM
February 12, 2004	Deadline for the March issue of the Databyte
February 13, 2004	Reservations due by noon for the February 18 ISACA dinner meeting
February 18, 2004	Chapter Meeting “Thesis: Security Concepts” – Rob Otten “Audits, Audit Work Papers, Discovery”
March 11, 2004	Deadline for the April issue of the Databyte
March 12, 2004	Reservations due by noon for the March 17 ISACA dinner meeting
March 17, 2004	Chapter Meeting <i>Student Night</i> “Panel Discussion on Skill Sets” “Disaster Communication Capacity/Planning” – Thomas Raupp
March 22 – March 24, 2004	ISACA/IIA Spring Seminar
March 31, 2004	Final Registration for June 2004 CISA and CISM
April 16, 2004	Reservations due by noon for the April 21 ISACA dinner meeting
April 20, 2004	Deadline for the May issue of the Databyte
April 21, 2004	Chapter Meeting “Lightweight Directory Access Protocol (LDAP) Audit Program” “Electric Choice and Energy Audits” – Joe McCormick
May 14, 2004	Reservations due by noon for the May 19 ISACA dinner meeting
May 19, 2004	Chapter Meeting “MS Access – How to Use in an Audit” – Mike Stolarczyk and Paul Haley
June 12, 2004	Above topic and speakers for both pre-dinner and after-dinner CISA and CISM exam

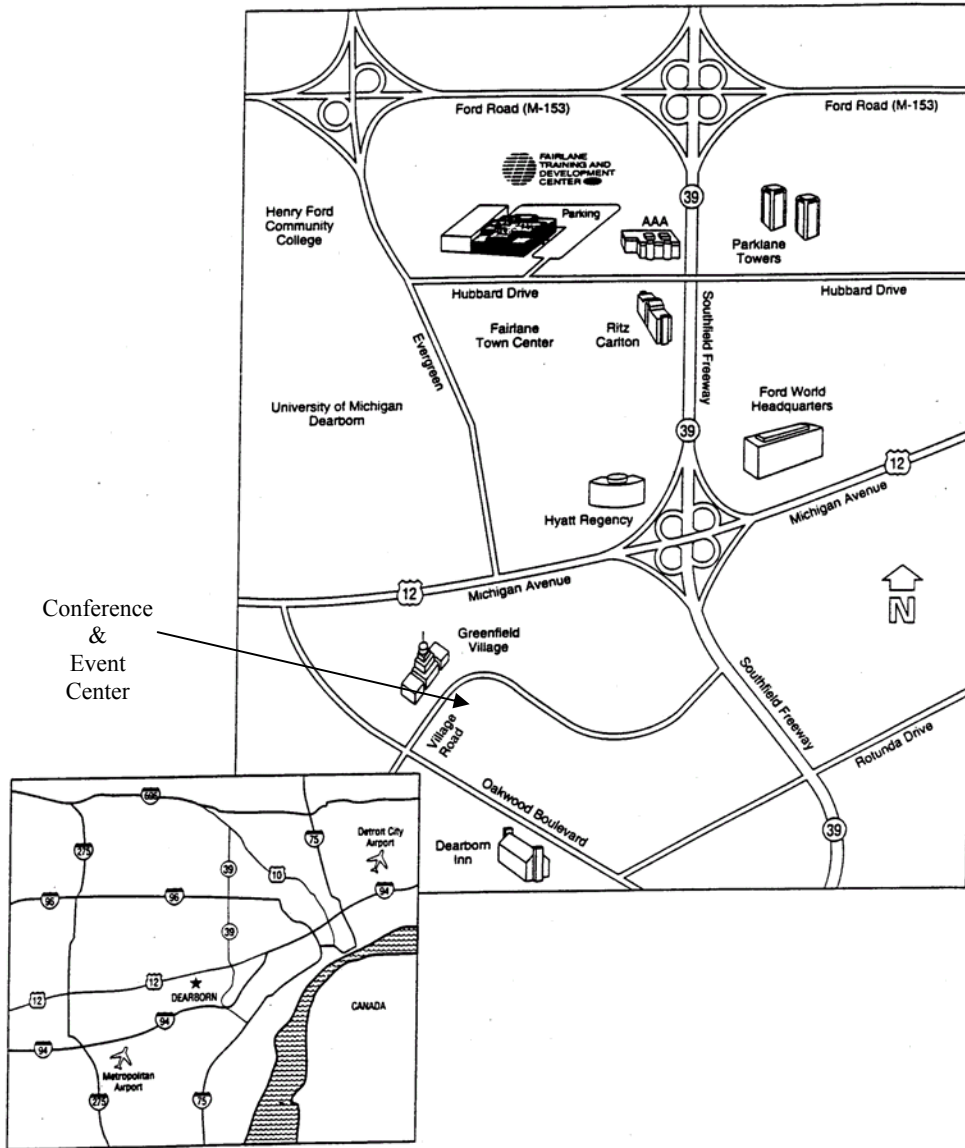
2004 Spring Seminar

March 22-24, 2004

The Detroit Chapters of the IIA and ISACA are proud to announce that we will again co-Chair the annual Spring Conference for the fifth year in a row. The 2004 Spring Conference has been designed to offer our members a local training opportunity at a very reasonable cost. This three-day event will offer six educational tracks on a variety of topics including Auditing of Core Business Operations, Power IT Audit, Risk Assessment, ACL, Control & Security of Telecommunications, Operating Systems, and Forensics, and, as always, sessions on the hot topics which impact our profession. We are very excited to announce that the 2004 event will be offered to our members at a cost of \$200 per day, no increase from the 2003 pricing.

Mark your calendar now for what has been a sell-out the last two years in a row!

FORD MOTOR COMPANY CONFERENCE & EVENT CENTER
1151 Village Road
Dearborn, MI 48124-5033
(313) 323-1972



FROM DETROIT METRO AIRPORT

Travel North East on Merriman. Take I-94 E ramp towards Detroit, merge onto I-94. Take US 24 North exit (Telegraph Rd.). Travel south to the US12 (Michigan Avenue) ramp. Turn right onto Michigan, then turn right onto Oakwood. Turn left on Village Road. The CEC is on the right.

FROM THE NORTH

Take M-39 South (Southfield Freeway) to the Michigan Avenue exit. Stay on the service drive to the first traffic light, which is Village Road. Turn right on Village, and the CEC is approximately 2 miles down on the left.

FROM THE SOUTH

Take M-39 North (Southfield Freeway) to the Rotunda exit. Stay on the service drive and turn left at the first intersection after crossing Rotunda. This is Village Road and the CEC is approximately 2 miles down on the left.

FROM THE EAST OR WEST

From Eastbound or Westbound I-94, take exit 206, Oakwood Blvd. Turn north on Oakwood, then in approximately 3 minutes, turn right on Village Road. The CEC is on the right.

FROM DOWNTOWN DETROIT

Take either I-94 West or US-10 (Lodge Freeway) to I-75 North. Take I-75 North to I-94 West. Take I-94 to exit 206, Oakwood Blvd. Turn north on Oakwood, then in approximately 3 minutes, turn right on Village Road. The CEC is on the right.

Risk Management

Written by Takisha Harper, Information Security Analyst, PPOM

It has been my experience that the more the merrier should not apply when developing a risk management team. The team should be a cross functional group that can fully represent the business but it is not strictly Information Technology's job, although IT should play a part. Risk Management itself has several key components including risk assessment (risk, control and recommendation analysis), sanction policy, audit, reporting and review. Incident Reporting and Response will feed some information into the risk management process but may be handled by another team. Risk management is a necessary tool for identifying, evaluating, and controlling risk, not eliminating them. No budget is big enough to eliminate all risks.

Risk Assessment

Asset inventory and analysis

The first stage in risk assessment is to identify assets. Assets can be tangible or non-tangible, meaning a server or a business process. For our purposes anything that assists the business in meeting its corporate goals or initiatives can be an asset to that company. Each asset should have a value tied to it based on its need by the company. This will allow a company to insure that all critical assets have been appropriately addressed. A large organization that has many assets could easily have some fall through the cracks and may need to do an asset inventory and valuation. In a small organization, all assets and processes may be weighted equally. It may be a misuse of time to assign values to each one. However by squaring the value of the asset and using the formula in this article, critical assets are more likely to be addressed in an effective and efficient manner. This can also prove invaluable for Business Continuity Planning and the documentation of critical assets.

Risk Analysis

Risk analysis identifies circumstances that may impede the ability of a department, a project, or the company to achieve its objectives. The process takes into consideration the controls currently in place, and determines the residual exposure if the vulnerabilities were exposed by a threat. Step one is to identify all threats and the associated vulnerabilities. Once the vulnerability is listed, an impact value (sometimes referred to as the vulnerability level) should be applied. This value will represent the impact that the vulnerability would have if it was exposed. Next the likelihood that the threat will occur should be calculated. The likelihood is focused on the threat, not the vulnerability, because the threat is the "TRIGGER" event. Risk can be defined by multiplying the impact value by the likelihood and adding the value of the asset squared (*if the asset valuation approach is used). $Risk = [A_x]^2 + [I_x \times L_{x1}]$

Control Analysis

In the control analysis, one wants to identify any areas that are considered high risk based on the risk analysis. A company can choose to address all vulnerabilities or only what they consider to be high risk. Again, if one uses the asset valuation method, it will better ensure that the most valuable assets are appropriately addressed. This is due to the fact that these assets will have higher risk values. The Control Analysis can identify possible controls or enhancements to current controls that could mitigate [not eliminate] vulnerabilities exposed by a particular threat. The control analysis is not intended to identify controls for mitigating the threat, but should focus on the mitigation of vulnerabilities and their impact. Once controls have been identified, the team will need to do a cost-benefit analysis of the controls and make appropriate recommendations.

Recommendation Analysis

In this stage, a recommendation should be made with regard to the controls that were identified. Again, this recommendation should be based on the cost-benefit analysis. The team may recommend to fully implement, partially implement, or not implement a control. This will need to be documented and submitted to management, who of course will have the option to agree or disagree with the team. Management should indicate in writing if they agree with the team's recommendation and this information should be stored for future use. However, if management disagrees with or alters a recommendation, the reasoning behind the decision should also be documented and stored. This stage may take considerable time and may necessitate management and the team getting together to discuss strategies.

Continued on Page 7

Continued from Page 6

Auditing

Auditing is a key in any compliance initiative. Auditing will allow a company to protect itself from issues that may not be caught or appropriately addressed via the risk assessment. Auditing also serves as a measure of compliance and helps to ensure that processes are being followed. One must also understand that the purpose of auditing is to ensure that the defined process is being followed. Whether the best process for the business is being followed will be determined by the review process.

Sanction

Sanctions give support or “teeth” to the recommendations approved by management. One must understand that some recommendations may impact an employee’s activities directly and this may not be readily accepted. If employees find out that there are no consequences when they break rules, they will pick and choose which rules they follow. Management should oversee the sanction policy, but HR should be the owner. This allows for a checks and balance process to be put into place. HR should be responsible for accepting, denying and carrying out recommendations from the Management about how to address an employee’s violations. The identification of these violations will stem from audits, reviews and vulnerability assessments done by Information Security. For example, during an audit, Information Security finds that an employee has been sending inappropriate e-mails. This would be reported to Management, and the manager would be responsible for working with HR to appropriately address the issue.

Reporting

For the most part, an efficient and effective Risk Management program must report findings good or bad in an appropriate time frame. Reporting allows decision makers to have the whole picture and make better decisions. Information Security’s effectiveness centers around reporting, sometimes called “tattling” by Information Technology professionals. Information Security doesn’t always have the power to make necessary changes, or apply sanctions as needed, but it has the ability to get the necessary information to the people who can.

Review

A company’s entire risk management program should be reviewed from time to time. This review will ensure that the most efficient and effective practices for the company’s environment are being used. Auditing, reporting, and sanctions will feed this process. However, in order to address possible conflicts of interest, it may be better to invite more objective individuals into the review process. This is the case because objectivity may be questioned if only the people who designed the whole process also review it.

Sources include: ISO17799, NIST, HIPAA, Perry Wilber for Kingsley IT security division

SENIOR INFORMATION TECHNOLOGY AUDITOR

The qualified candidate will develop, plan and perform independent audits of information systems and technical infrastructures, processes, data centers and computer operations to evaluate internal controls and ensure compliance to established policies, standards, procedures and security requirements. You will also provide internal consulting in system development projects and other critical IT initiatives, as you partner with IT and Business management.

A Bachelor’s degree in Business Administration, Computer Science or a related field and CISA designation are required. Proven experience with a programming language and in data extraction/analysis is desired. Demonstrated audit skills in system development projects, information security, mainframe and distributed computing environments are desired.

The Auto Club Group offers a competitive salary and generous benefits package, including medical, dental, vision, 401(k), pension and much more. If you want to join an audit team that is valued by management and a company that wants to be the best in the marketplace, please send your resume and salary requirements to: **Jeff DePoorter, Staffing Dept., AAA Michigan, 1 Auto Club Drive, Dearborn, MI 48126, FAX (313) 436-7188 or e-mail to: jgdepoorter@aaamichigan.com**

The Auto Club Group is an
Equal Opportunity Employer

Monthly Highlights

December 4, 2003
December 9, 2003

Reservations due by 6:00 p.m. for the December 9 ISACA/IIA dinner meeting
Chapter Meeting

(Please Note: This meeting is on the Second Tuesday of the month instead of the Third Wednesday and the location and starting time are different.)

Joint meeting with the IIA

“HIPAA” – Fred Heller, Director of Technology, Jefferson Wells International

“Audit Committee Perspective – What’s Changed?” – Eric Hespenheide, Partner, Deloitte & Touche LLP

December 9, 2003

Deadline for the January issue of the Databyte

Menu – December 9, 2003

DINNER BUFFET

MEDITERRANEAN SALAD

Artichoke hearts, feta cheese, black olives and red onion tossed with romaine lettuce and balsamic vinaigrette

CHILEAN SEA BASS pan-seared and served with Beurre Blanc Sauce

CHAR-GRILLED CHICKEN with Gemelli Pasta served with olive oil, garlic, and pesto

POTATO PANCAKES

STEAMED BROCCOLI

THREE BERRY CRISP

served with Vanilla Ice Cream



The Chapter must provide the number of reservations by 6:00 p.m. on the Thursday before the meeting. To ensure that we can accommodate those who wish to attend and the facility can provide the best service possible, please make your reservations early. If you have made a reservation and cannot attend, please call Suzanne McCormick at (248) 471-3075. Your cooperation is greatly appreciated.

New Detroit Chapter Members

Maninder Bharadwaj

Ercel Kaan

DATABYTE



Information Systems
Audit and Control
Association

DETROIT AREA CHAPTER

SUZANNE McCORMICK, EDITOR

30032 FINK AVENUE

FARMINGTON HILLS, MI 48336

(248) 471-3075

Jsmccor65@aol.com